SANbox2-16 Fibre Channel Switch

Installation Guide

Information furnished in this manual is believed to be accurate and reliable. However, QLogic Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which may result from its use. QLogic Corporation reserves the right to change product specifications at any time without notice. Applications described in this document for any of these products are for illustrative purposes only. QLogic Corporation makes no representation nor warranty that such applications are suitable for the specified use without further testing or modification. QLogic Corporation assumes no responsibility for any errors that may appear in this document.

QLogic, SANbox, SANbox2, SANblade, SANsurfer, and Multistage are trademarks or registered trademarks of QLogic Corporation.

Java and Solaris are registered trademarks of Sun Microsystems, Inc.

Pentium is a registered trademark of Intel Corporation.

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows NT, and Windows 2000, and Internet Explorer are registered trademarks of Microsoft Corporation.

Netscape Navigator is a registered trademark of Netscape Communications Corporation.

Red Hat is a registered trademark of Red Hat Software Inc.

SANmark is a registered trademark of the Fibre Channel Industry Association.

All other brand and product names are trademarks or registered trademarks of their respective owners.

Document Revision History

Revision A, Release, September 2003

© 2000–2003 QLogic Corporation
First Printed: May 2001
All Rights Reserved Worldwide.
Printed in U.S.A.

Table of Contents

Section 1 Introduction

1.1 Intended Audience 1-1
1.2 Related Materials 1-2
1.3 Safety Notices 1-3
1.4 Sicherheitshinweise 1-3
1.5 Notes informatives relatives à la sécurité 1-3
1.6 Communications Statements 1-4
1.6.1 Federal Communications Commission (FCC) Class A Statement 1-4
1.6.2 Canadian Department of Communications Class A Compliance Statement 1-4
1.6.3 Avis de conformité aux normes du ministère des Communications du Canada 1-4
1.6.4 CE Statement 1-5
1.6.5 VCCI Class A Statement 1-6
1.6.6 BSMI Class A Statement 1-6
1.7 Laser Safety Information 1-7
1.8 Electrostatic Discharge Sensitivity (ESDS) Precautions 1-7
1.9 Accessible Parts 1-8
1.10 Pièces Accessibles 1-8
1.11 Zugängliche Teile 1-8
1.12 General Public License 1-9
1.12.1 Preamble 1-9
1.12.2 Terms And Conditions For Copying, Distribution And Modification 1-10
1.12.3 How to Apply These Terms to Your New Programs 1-14
1.13 Technical Support 1-16
1.13.1 Availability 1-16
1.13.2 Training 1-16
1.13.3 Contact Information 1-16

Section 2 General Description

2.1 Chassis Controls and LEDs 2-2
2.1.1 Power Switches 2-2
2.1.2 Maintenance Button 2-2
2.1.3 Chassis LEDs 2-3
2.1.3.1 Over Temperature LED (Amber) 2-3
2.1.3.2 Fan Fail LED (Amber) 2-3

2.1.3.3 Heartbeat LED (Amber) 2-4
2.1.3.4 Input Power LED (Green) 2-4
2.2 Fibre Channel Ports 2-4
2.3 Port LEDs 2-5
2.3.0.5 Logged-In LED 2-5
2.3.0.6 Activity LED 2-5
2.3.1 Small Form-Factor Pluggable (SFP) Transceivers 2-6
2.3.1.1 Port Modes 2-6
2.3.1.2 Fabric Ports 2-7
2.3.1.3 Expansion Port 2-7
2.4 Ethernet Port 2-7
2.5 Serial Port 2-8
2.6 Power Supplies 2-9
2.7 Fans 2-10
2.8 Switch Management 2-10

Section 3 Planning

3.1 Devices 3-1
3.2 Multiple Chassis Fabrics 3-2
3.2.1 Domain ID, Principal Priority, and Domain ID Lock 3-2
3.2.2 Common Topologies 3-3
3.2.2.1 Cascade Topology 3-3
3.2.2.2 Mesh Topology 3-4
3.2.2.3 Multistage Topology 3-5
3.3 Performance 3-6
3.3.1 Distance 3-6
3.3.2 Bandwidth 3-7
3.3.3 Latency 3-7
3.4 Device Access 3-8
3.4.1 Soft Zones 3-9
3.4.2 Access Control List Hard Zones 3-9
3.4.3 Virtual Private Fabric Hard Zones 3-10
3.4.4 User Account Security 3-11
3.4.5 Device Security 3-11
3.4.5.1 Security Example: Switches and HBAs 3-12
3.4.5.2 Security Example: Host Authentication 3-14
3.4.6 Fabric Services 3-15
3.5 Fabric Management 3-16

Section 4 Installation

4.1 Site Requirements 4-1
4.1.1 Fabric Management Workstation 4-1
4.1.2 Switch Power Requirements 4-1
4.1.3 Environmental Conditions 4-2
4.2 Installing a Switch 4-2
4.2.1 Mount the Switch 4-3
4.2.2 Install SFP Transceivers 4-5
4.2.3 Connect the Switch to AC Power 4-6
4.2.4 Connect the Management Workstation to the Switch 4-9
4.2.4.1 Ethernet Connection 4-10
4.2.4.2 Serial Connection 4-10
4.2.5 Install SANbox Manager 4-11
4.2.6 SANsurfer Management Suite Disk - Windows Installation 4-12
4.2.7 SANsurfer Management Suite Disk - Linux Installation 4-12
4.2.8 SANsurfer Management Suite Disk - Solaris Installation 4-13
4.2.9 SANbox2 Installation Disk - Windows Installation 4-14
4.2.10 SANbox2 Installation Disk - Linux Installation 4-15
4.2.10.1 SANbox2 Installation Disk - Solaris Installation 4-15
4.2.11 Configure the Switch 4-15
4.2.12 Configure the Ports 4-16
4.2.13 Cable Devices to the Switch 4-16
4.3 Install Firmware 4-17
4.3.1 Using SANbox Manager to Install Firmware 4-17
4.3.2 Using the CLI to Install Firmware 4-18
4.3.3 Using FTP and the CLI to Install Firmware 4-19
4.4 Powering Down a Switch 4-20

Section 5 Diagnostics/Troubleshooting

5.1 POST Diagnostics 5-1
5.1.1 Heartbeat LED Blink Patterns 5-1
5.1.1.1 Normal (all pass) 5-1
5.1.1.2 Maintenance Mode Pattern 5-2
5.1.1.3 Internal Firmware Failure Blink Pattern 5-2
5.1.1.4 Fatal Error Blink Pattern 5-2
5.1.1.5 Configuration File System Error Blink Pattern 5-2
5.1.2 Logged-In LED Indications 5-5
5.1.2.1 E_Port Isolation 5-6
5.1.2.2 Excessive Port Errors 5-7
5.2 Chassis Diagnostics 5-9

5.2.1 Chassis Over Temperature LED is Illuminated 5-10
5.2.2 Input Power LED Is Extinguished 5-10
5.2.3 Fan Fail LED is Illuminated 5-10
5.2.4 Output Power LED Is Extinguished 5-11
5.2.5 Power Supply Over Temperature LED is Illuminated 5-11
5.3 Recovering a Switch 5-12
5.3.1 Maintenance – Exit 5-13
5.3.2 Maintenance – Image Unpack 5-14
5.3.3 Maintenance – Reset Network Config 5-14
5.3.4 Maintenance – Reset Password File 5-14
5.3.5 Maintenance – Copy Log Files 5-14
5.3.6 Maintenance – Remove Switch Config 5-14
5.3.7 Maintenance – Remake Filesystem 5-15
5.3.8 Maintenance – Reset Switch 5-15
5.3.9 Maintenance – Show Firmware Versions 5-15
5.3.10 Maintenance – Set Active Image 5-15

Section 6 Removal/Replacement

6.1 SFP Transceivers 6-2
6.2 Power Supplies 6-3
6.3 Fans 6-4

Appendix A Specifications

A.1 Fabric Specifications A-1
A.2 Maintainability A-2
A.3 Fabric Management A-3
A.4 Dimensions A-3
A.5 Electrical A-3
A.6 Environmental A-4
A.7 Regulatory Certifications A-5
A.8 Shortwave Laser SFP 1G/2G (multi-mode) A-6
A.9 Longwave Laser SFP 1G/2G (single-mode) A-7

Appendix B Command Line Interface

B.1 Logging On to a Switch B-1
B.2 Command Syntax B-2
B.3 Commands B-3
Admin Command B-4
Alias Command B-5
Config Command B-7

Date Command B-10
Fallback Command B-11
Group Command B-12
Hardreset Command B-16
Help Command B-17
History Command B-19
Hotreset Command B-20
Image Command B-21
Lip Command B-22
Passwd Command B-23
Ping Command B-24
Ps Command B-25
Quit Command B-26
Reset Command B-27
Security Command B-32
Securityset Command B-35
Set Command B-37
Set Config Command B-39
Set Log Command B-50
Set Port Command B-53
Set Setup Command B-54
Show Command B-59
Show Config Command B-72
Show Log Command B-75
Show Perf Command B-77
Show Setup Command B-79
Shutdown Command B-82
Test Command B-83
Uptime Command B-86
User Command B-87
Whoami Command B-90
Zone Command B-91
Zoneset Command B-95
Zoning Command B-97

Glossary

Index

Figures

Figure		Page
2-1	SANbox2-16 Fibre Channel Switch	2-1
2-2	Chassis Controls and LEDS	2-2
2-3	Chassis LEDs	2-3
2-4	Fibre Channel Ports	2-4
2-5	Port LEDs	2-5
2-6	SFP Transceiver	2-6
2-7	Ethernet Port	2-7
2-8	Serial Port and Pin Identification	2-8
2-9	Power Supply Components	2-9
2-10	Fans	2-10
3-1	Cascade-with-a-Loop Topology	3-3
3-2	Mesh Topology	3-4
3-3	Multistage Topology	3-5
3-4	Security Example: Switches and HBAs	3-12
3-5	Security Example: Management Server	3-14
4-1	SANbox2-16 Fibre Channel Switch	4-2
4-2	Installing Rack Mount Brackets	4-5
4-3	Ethernet and Serial Cable Connections	4-9
5-1	Logged-In LED	5-5
5-2	Logged-In LED Indications	5-5
5-3	Chassis and Power Supply LEDs	5-9
6-1	SFP Transceiver Installation	6-2
6-2	Power Supply Removal	6-3
6-3	Fan Removal	6-4
6-4	Fan Installation for Switch Model SB2A-16B	6-5

Tables

Table		Page
2-1	Serial Port Pin Identification	2-8
3-1	Port-to-Port Transmission Combinations	3-7
3-2	Port-to-Port Latency	3-7
4-1	Management Workstation Requirements	4-1
B-1	Command-Line Completion	B-2
B-2	Commands Listed by Authority Level	B-3
B-3	Group Member Attributes	B-12
B-4	Group Member Attributes	B-13
B-5	Switch Configuration Defaults	B-28
B-6	Port Configuration Defaults	B-28
B-7	Alarm Threshold Configuration Defaults	B-29
B-8	Zoning Configuration Defaults	B-30
B-9	SNMP Configuration Defaults	B-30
B-10	System Configuration Defaults	B-31
B-11	Security Configuration Defaults	B-31
B-12	Set Config Port Parameters	B-39
B-13	Security Configuration Parameters	B-41
B-14	Set Config Switch Parameters	B-42
B-15	Set Config Threshold Parameters	B-44
B-16	Set Config Zoning Parameters	B-45
B-17	SNMP Configuration Settings	B-54
B-18	System Configuration Settings	B-55
B-19	Show Port Parameters	B-61

Notes

Section 1

Introduction

This manual describes the features and installation of the SANbox2-16 Fibre Channel switch, firmware version 3.0. This manual is organized as follows:

- Section 1 describes the intended audience, related materials, safety notices, communications statements, laser safety information, electrostatic discharge sensitivity precautions, accessible parts, general program license, and technical support.
- Section 2 is an overview of the switch. It describes indicator LEDs and all user controls and connections.
- Section 3 describes the factors to consider when planning a fabric.
- Section 4 explains how to install and configure the switch.
- Section 5 describes the diagnostic methods and troubleshooting procedures.
- Section 6 describes the removal/replacement procedures for all field replaceable units (FRUs).
- Appendix A lists the switch specifications.
- Appendix B describes the Command Line Interface.

Please read the communications statements and laser safety information later in this section. Use this manual with the *SANbox2-8c/16 Switch Management User's Guide*.

1.1 Intended Audience

This manual introduces users to the switch and explains its installation and service. It is intended for users who are responsible for installing and servicing network equipment.

1.2 Related Materials

The following manuals and materials are referenced in the text and/or provide additional information.

- *SANbox2-8c/16 Switch Management User's Guide*, Publication Number 59022-07.
- Fibre Channel-Arbitrated Loop (FC-AL-2) Rev. 6.8.
- Fibre Channel-10-bit Interface Rev. 2.3.
- Definitions of Managed Objects for the Fabric Element in Fibre Channel Standard (draft-ietf-ipfc-fabric-element-mib-04.txt).

The Fibre Channel Standards are available from:

Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112-5776 Phone: (800) 854-7179 or (303) 397-7956
Fax: (303) 397-2740.

1.3 Safety Notices

A **Warning** notice indicates the presence of a hazard that has the potential of causing personal injury.

4-3, 4-6, 6-1

A **Caution** notice indicates the presence of a hazard that has the potential of causing damage to the equipment.

4-4, 5-15, 6-4

1.4 Sicherheitshinweise

Ein **Warnhinweis** weist auf das Vorhandensein einer Gefahr hin, die möglicherweise Verletzungen zur Folge hat.

4-3, 4-7, 6-1

Ein **Vorsichtshinweis** weist auf das Vorhandensein einer Gefahr hin, die möglicherweise Geräteschäden zur Folge hat.

4-4, 5-15, 6-4

1.5 Notes informatives relatives à la sécurité

Une note informative **Avertissement** indique la présence d’un risque pouvant entraîner des blessures.

4-3, 4-6, 6-1

Une note informative **Attention** indique la présence d’un risque pouvant entraîner des dégâts matériels.

4-4, 5-15, 6-4

1.6 Communications Statements

The following statements apply to this product. The statements for other products intended for use with this product appear in their accompanying manuals.

1.6.1 Federal Communications Commission (FCC) Class A Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause unacceptable interference, in which case the user will be required to correct the interference at their own expense.

Neither the provider nor the manufacturer is responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

1.6.2 Canadian Department of Communications Class A Compliance Statement

This equipment does not exceed Class A limits for radio emissions for digital apparatus, set out in Radio Interference Regulation of the Canadian Department of Communications. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps necessary to correct the interference.

1.6.3 Avis de conformité aux normes du ministère des Communications du Canada

Cet équipement ne dépasse pas les limites de Classe A d'émission de bruits radioélectriques por les appareils numériques, telles que prescrites par le Réglement sur le brouillage radioélectrique établi par le ministère des Communications du Canada. L'exploitation faite en milieu résidentiel peut

entraîner le brouillage des réceptions radio et télé, ce qui obligerait le propriétaire ou l'opérateur à prendre les dispositions nécwssaires pour en éliminer les causes.

1.6.4
CE Statement

The CE symbol on the equipment indicates that this system complies with the EMC (Electromagnetic Compatibility) directive of the European Community (89/336/EEC) and to the Low Voltage (Safety) Directive (73/23/EEC). Such marking indicates that this system meets or exceeds the following technical standards:

- EN60950/A11:1997 – “Safety of Information Technology Equipment, Including Electrical Business Equipment”.
- EN55022:1998 – “Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment”.
- EN55024-1:1998 – “Electromagnetic compatibility - Generic immunity standard Part 1: Residential commercial, and light industry.”
  - IEC1000-4-2:1995 – “Electrostatic Discharge Immunity Test”
  - IEC1000-4-3:1995 – “Radiated, Radio-Frequency, Electromagnetic Field Immunity Test”
  - IEC1000-4-4:1995 – “Electrical Fast Transient/Burst Immunity Test”
  - IEC1000-4-5:1995 – “Surge Immunity Test”
  - IEC1000-4-6:1996 – “Immunity To Conducted Disturbances, Induced By Radio-Frequency Fields”
  - IEC1000-4-8:1993 – "Power Frequency Magnetic Field Immunity Test”
  - IEC1000-4-11:1994 – “Voltage Dips, Short Interruptions And Voltage Variations Immunity Tests”
- EN61000-3-2:1995 – “Limits For Harmonic Current Emissions (Equipment Input Current Less Than/Equal To 16 A Per Phase)” Class A
- EN61000-3-3:1995 – “Limitation Of Voltage Fluctuations And Flicker In Low-Voltage Supply Systems For Equipment With Rated Current Less Than Or Equal To 16 A”

1.6.5
VCCI Class A Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council For Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

1.6.6
BSMI Class A Statement

警告使用者:

這是甲類的資訊產品, 在居住的環境中使用時, 可能會造成射頻干擾, 在這種情況下, 使用者會被要求採取某些適當的對策.

Warning:

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user will be required to take adequate measures.

1.7

Laser Safety Information

This product may use Class 1 laser optical transceivers to communicate over the fiber optic conductors. The U.S. Department of Health and Human Services (DHHS) does not consider Class 1 lasers to be hazardous. The International Electrotechnical Commission (IEC) 825 Laser Safety Standard requires labeling in English, German, Finnish, and French stating that the product uses Class 1 lasers. Because it is impractical to label the transceivers, the following label is provided in this manual.

1.8

Electrostatic Discharge Sensitivity (ESDS) Precautions

The assemblies used in the switch chassis are ESD sensitive. Observe ESD handling procedures when handling any assembly used in the switch chassis.

1.9 Accessible Parts

The Field Replaceable Units (FRUs) in the SANbox2-16 switch are the following:

- Small Form-Factor Pluggable (SFP) optical transceivers
- Power supplies
- Fans

Refer to Section 6 Removal/Replacement for more information.

1.10 Pièces Accessibles

Les pièces remplaçables, Field Replaceable Units (FRU), du commutateur SANbox2-16 Fibre Channel Switch sont les suivantes:

- Interfaces aux media d'interconnexion appelés SFP transceivers.
- Alimentations de courant
- Ventilateurs

Se reporter à la Section 6 (Procédures de retrait et remplacement) pour plus de renseignements.

1.11 Zugängliche Teile

Nur die folgenden Teile im SANbox2-16 Fibre Channel Switch können kundenseitig ersetzt werden:

- Schnittstellen für die Zwischenverbindungsträger, SFP transceivers genannt.
- Netzteile
- Gehäuselüfte

Weitere Informationen finden Sie im Abshcnitt 6 (Ausbauen der ersetzbaren Teile).

1.12 General Public License

QLogic Fibre Channel switches are powered by the Linux operating system. A machine-readable copy of the Linux source code is available upon written request to the following address. A nominal fee will be charged for reproduction, shipping, and handling costs in accordance with the General Public License.

QLogic Corporation
6321 Bury Drive
Eden Prairie, MN 55346-1739
Attention: Technical Support - Source Request

Warning: Installation of software or files not authorized by QLogic will immediately and irrevocably void all warranty and service contracts on the affected units.

The following general public license has been reproduced with permission from:

GNU General Public License
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

1.12.1 Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

1.12.2
Terms And Conditions For Copying, Distribution And Modification

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such

modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the

rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

11. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this

License, you may choose any version ever published by the Free Software Foundation.

12. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

13. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

14. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

1.12.3
How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) *yyyy name of author*

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright (C) *year name of author*

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

> *signature of Ty Coon*, 1 April 1989
> Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

1.13 Technical Support

Customers should contact their authorized maintenance provider for technical support of their QLogic switch products. QLogic-direct customers may contact QLogic Technical Support; others will be redirected to their authorized maintenance provider.

Visit the QLogic support Web site listed in Contact Information for the latest firmware and software updates.

1.13.1 Availability

QLogic Technical Support is available from 7:00 AM to 7:00 PM Central Standard Time, Monday through Friday, excluding QLogic-observed holidays.

1.13.2 Training

QLogic offers certification training for the technical professional for both the SANblade HBAs and the SANbox2 switches. From the training link at www.qlogic.com, you may choose Electronic-Based Training or schedule an intensive "hands-on" Certification course.

Technical Certification courses include installation, maintenance and troubleshooting QLogic SAN products. Upon demonstrating knowledge using live equipment, QLogic awards a certificate identifying the student as a Certified Professional. The training professionals at QLogic may be reached by email at tech.training@qlogic.com.

1.13.3 Contact Information

Address:	QLogic Switch Products Inc. 6321 Bury Drive Eden Prairie, Minnesota 55346 USA
Telephone:	+1 952-932-4040
Fax:	+1 952-932-4018
Email: Technical Service Technical Training	 support@qlogic.com tech.training@qlogic.com
Switch Support Web Site:	http://support.qlogic.com

Section 2
General Description

This section describes the features and capabilities of the SANbox2-16 Fibre Channel switch. The following topics are described:

- Chassis controls and LEDs
- Fibre channel ports
- Ethernet port
- Serial port
- Power supplies
- Fans
- Switch management

Fabrics are managed with the SANbox Manager switch management application (version 3.00) and the Command Line Interface (CLI). Refer to the *SANbox2-8c/16 Switch Management User's Guide* for information about using the SANbox Manager application. Refer to Appendix B Command Line Interface for more information about the command line interface.

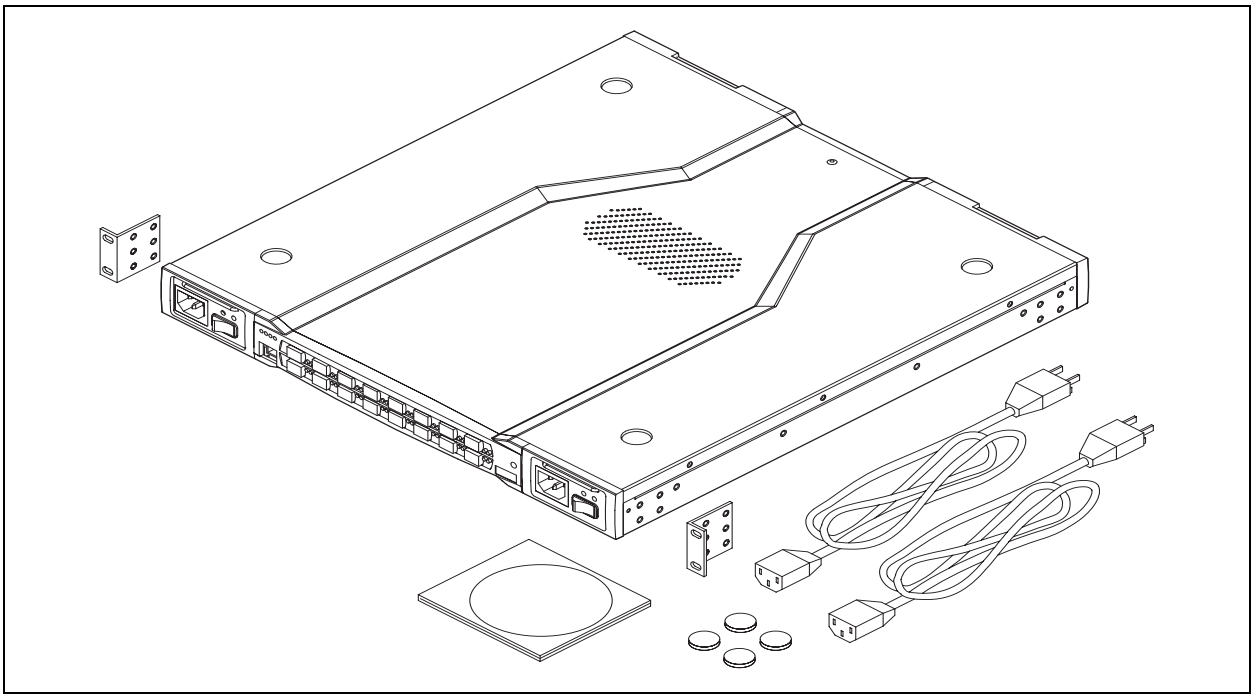


Figure 2-1. SANbox2-16 Fibre Channel Switch

2.1 Chassis Controls and LEDs

Chassis controls include the power supply On/Off switches and the Maintenance button as shown in Figure 2-2. The Maintenance button is used to recover a disabled switch. The chassis LEDs provide information about the switch's operational status. The chassis LEDs include the Over Temperature LED, Fan Fail LED, Heartbeat LED, and the Input Power LED.

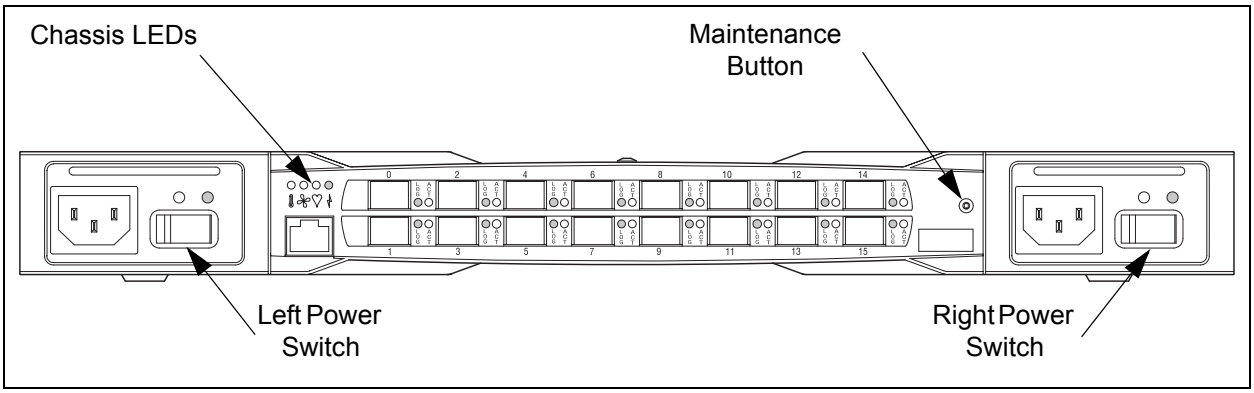


Figure 2-2. Chassis Controls and LEDS

2.1.1 Power Switches

Each power supply has an On/Off switch that controls power to the switch logic circuitry. To apply power to the switch, place both switches in the On position.

2.1.2 Maintenance Button

The Maintenance button is a momentary switch on the front panel. Its purpose is to place the switch in maintenance mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes when flash memory or the resident configuration file is corrupted. Refer to "Recovering a Switch" on page 5-12 for information about maintenance mode.

To place the switch in maintenance mode, do the following:

1. Isolate the switch from the fabric. Open a Telnet session, and enter the Shutdown command. Refer to "Shutdown Command" on page B-82.
2. Place both power supply switches in the Off position.
3. Press and hold the Maintenance button with a pointed tool, then place one of the power supply switches in the On position. You can release the Maintenance button after the Input Power LED illuminates. When the switch is in maintenance mode, the Heartbeat LED illuminates continuously. Refer

to ”Chassis LEDs” on page 2-3 for information about the Input Power LED and the Heartbeat LED.

To return to normal operation, power cycle the switch.

2.1.3
Chassis LEDs

The chassis LEDs shown in Figure 2-3 provide status information about switch operation. Refer to ”Port LEDs” on page 2-5 for information about port LEDs. Refer to ”Power Supplies” on page 2-9 for information about power supply LEDs.

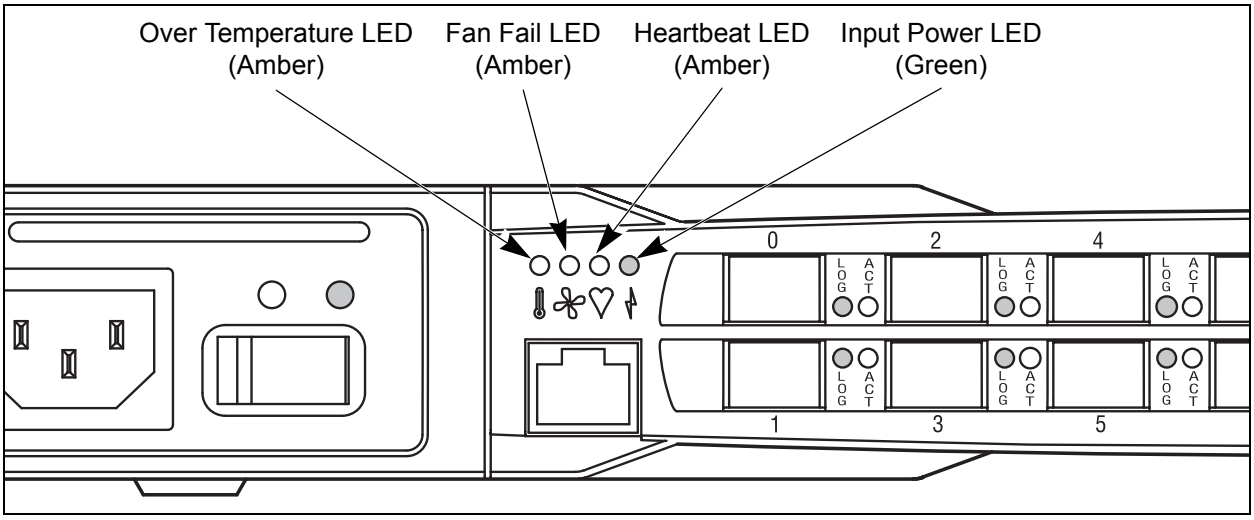


Figure 2-3. Chassis LEDs

2.1.3.1
Over Temperature LED (Amber)

The Over Temperature LED provides status information about the air temperature inside the switch. This LED illuminates to indicate that the switch logic circuitry is overheating. Refer to Section 5 Diagnostics/Troubleshooting for information about troubleshooting over temperature conditions.

2.1.3.2
Fan Fail LED (Amber)

The Fan Fail LED indicates operational status of all fans. This LED illuminates if the speed of any fan falls below the normal range. Removing a fan will not illuminate the Fan Fail LED. Refer to Section 5 Diagnostics/Troubleshooting for information about troubleshooting fan failure conditions.

2.1.3.3
Heartbeat LED (Amber)

The Heartbeat LED indicates the status of the internal switch processor and the results of the Power On Self Test (POST). Following a normal power-up, the Heartbeat LED blinks about once per second to indicate that the switch passed the POST and that the internal switch processor is running. In maintenance mode, the Heartbeat LED illuminates continuously. Refer to ”Heartbeat LED Blink Patterns” on page 5-1 for more information about Heartbeat LED blink patterns.

2.1.3.4
Input Power LED (Green)

The Input Power LED indicates the voltage status at the switch logic circuitry. This LED illuminates when the switch logic circuitry is receiving the proper DC voltages.

2.2
Fibre Channel Ports

The SANbox2-16 switch has 16 Fibre Channel ports numbered 0–15 as shown in Figure 2-4. Each of these ports is served by a Small Form-Factor Pluggable (SFP) optical transceiver. The port LEDs are located to the right of their respective ports and provide port login and activity status information. The ports self discover the proper mode when connected to public devices and other switches.

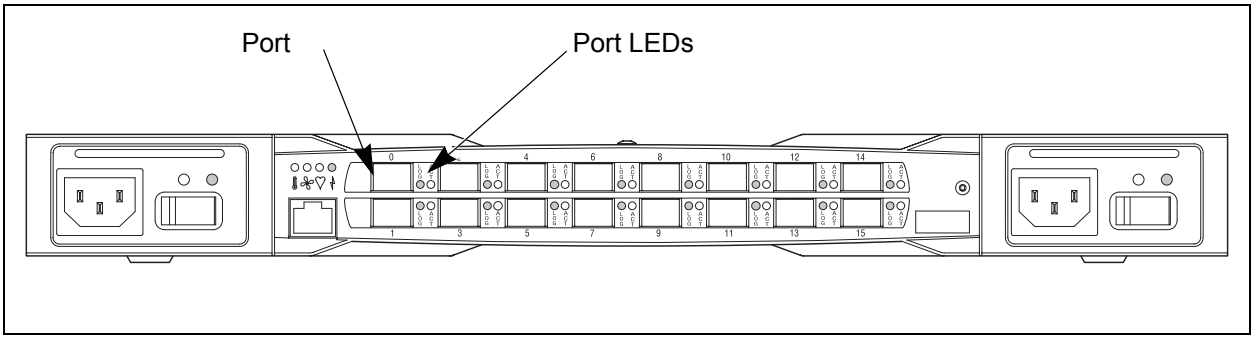


Figure 2-4. Fibre Channel Ports

2.3
Port LEDs

Each Fibre Channel port has its own Logged-In LED and Activity LED as shown in Figure 2-5.

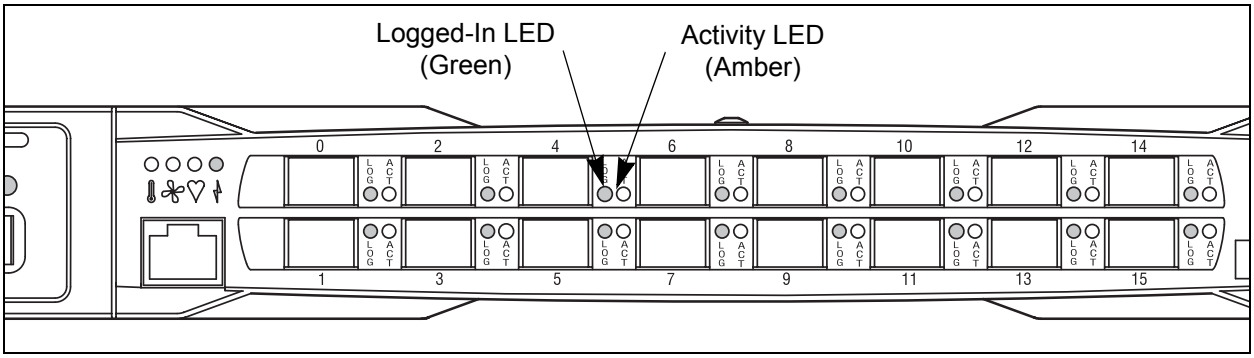


Figure 2-5. Port LEDs

2.3.0.5
Logged-In LED

The Logged-in LED indicates the logged-in or initialization status of the connected devices. After successful completion of the POST, the switch extinguishes all Logged-In LEDs. Following a successful loop initialization or port login, the switch illuminates the corresponding logged-in LED. This shows that the port is properly connected and able to communicate with its attached devices. The Logged-In LED remains illuminated as long as the port is initialized or logged in. If the port connection is broken or an error occurs that disables the port, the Logged-In LED will flash. Refer to ”Logged-In LED Indications” on page 5-5 for more information about the Logged-In LED.

2.3.0.6
Activity LED

The Activity LED indicates that data is passing through the port. Each frame that the port transmits or receives causes this LED to illuminate for 50 milliseconds. This makes it possible to observe the transmission of a single frame. When extending credits, the Activity LED for a donor port will reflect the traffic of the recipient port. Refer to ”Distance” on page 3-6 for more information about extended credits and donor ports.

2.3.1
Small Form-Factor Pluggable (SFP) Transceivers

An SFP transceiver, like the one shown in Figure 2-6, converts electrical signals to and from optical laser signals to transmit and receive data. SFP transceivers plug into the ports; duplex fiber optic cables plug into the transceivers which then connect to the devices. A port is capable of transmitting at 1 Gbps or 2 Gbps; however, the transceiver must be capable of 2 Gbps for the port to deliver at that rate.

The SFP transceivers are hot swappable. This means that you can remove or install an SFP transceiver while the switch is operating without harming the switch or the transceiver. However, communication with the connected device will be interrupted. Refer to ”SFP Transceivers” on page 6-2 for information about installing and removing SFP optical transceivers.

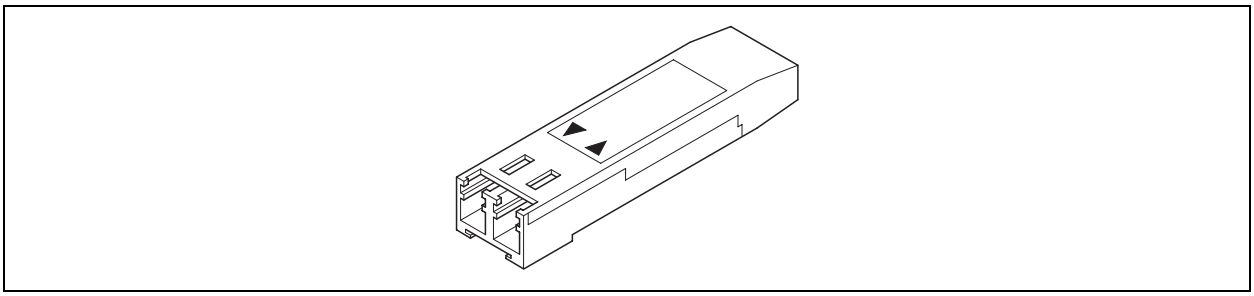


Figure 2-6. SFP Transceiver

2.3.1.1
Port Modes

SANbox2-16 switches support the following port modes:

- Generic ports (GL_Port and G_Port)
- Fabric ports (FL_Port and F_Port)
- Expansion ports (E_Port)

Switches come from the factory with all ports configured as GL_Ports. GL_Ports self-configure in the following ways:

- FL_Port when connected to a loop of public devices
- F_Port when connected to a single public device. If the device is a single device on a loop, the GL_Port will attempt to configure first as an F_Port, then if that fails, as an FL_Port.
- E_Port when connected to another FC-SW-2 compliant switch

G_Ports self-configure in the following ways:

- F_Port when connected to a public device
- E_Port when connected to another FC-SW-2 compliant switch

Refer to the *SANbox2-8c/16 Switch Management User's Guide* for more information about defining port modes.

2.3.1.2
Fabric Ports

An FL_Port can support a loop of up to 126 public devices. An FL_Port can also configure itself during the fabric login process as an F_Port when connected to a single public device (N_Port).

2.3.1.3
Expansion Port

E_Ports enable you to expand the fabric by connecting SANbox2-16 switches with other FC-SW-2 compliant switches. SANbox2-16 switches self-discover all inter-switch connections. Refer to "Multiple Chassis Fabrics" on page 3-2 for more information about multiple chassis fabrics.

2.4
Ethernet Port

The Ethernet port shown in Figure 2-7 is an RJ-45 connector that provides a connection to a management workstation. A management workstation can be a Windows, Solaris™, or a Linux® workstation that is used to configure and manage the switch fabric. You can manage the switch over an Ethernet connection using SANbox Manager, the Command Line Interface (CLI), or SNMP. The switch through which the fabric is managed is called the fabric management switch.

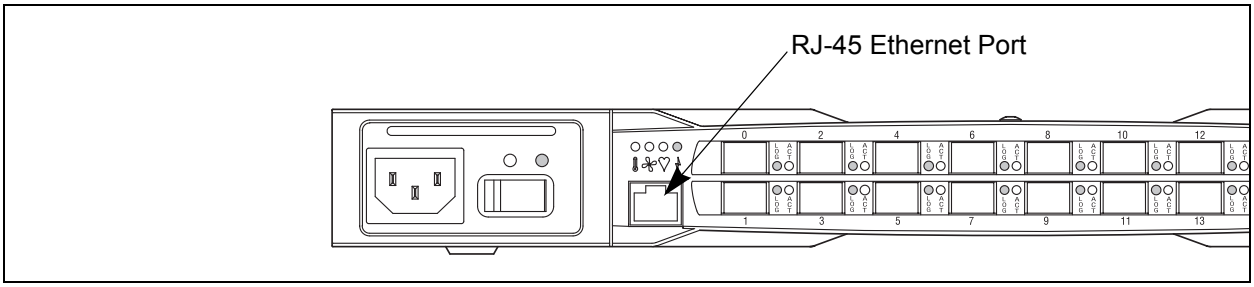


Figure 2-7. Ethernet Port

2.5 Serial Port

The SANbox2-16 switch is equipped with an RS-232 serial port for maintenance purposes. The serial port location is shown in Figure 2-8. You can manage the switch through the serial port using the CLI.

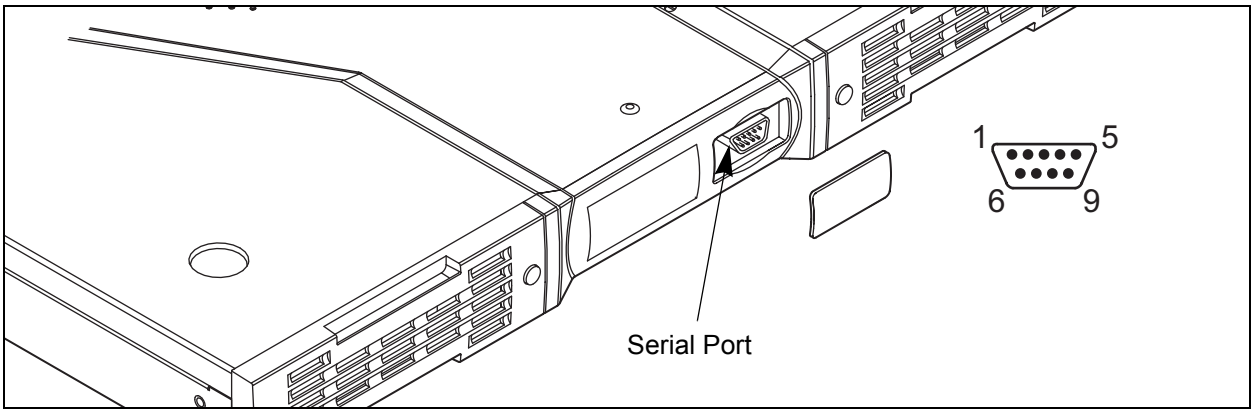


Figure 2-8. Serial Port and Pin Identification

The serial port connector requires a null-modem F/F DB9 cable. The pins on the switch RS-232 connector are shown in Figure 2-8 and identified in Table 2-1. Refer to ”Connect the Management Workstation to the Switch” on page 4-9 for information about connecting the management workstation through the serial port.

Table 2-1. Serial Port Pin Identification

Pin Number	Description
1	Carrier Detect (DCD)
2	Receive Data (RxD)
3	Transmit Data (TxD)
4	Data Terminal Ready (DTR)
5	Signal Ground (GND)
6	Data Set Ready (DSR)
7	Request to Send (RTS)
8	Clear to Send (CTS)
9	Ring Indicator (RI)

2.6 Power Supplies

The power supplies convert standard 110 or 230 VAC to DC voltages for the various switch circuits. Each power supply has an AC power receptacle, an On/Off switch, and two status LEDs as shown in Figure 2-9. After connecting a power supply to an AC voltage source and placing the power switch in the On position, the power supply is energized and DC voltage is delivered to the switch logic circuitry. Refer to Section 6 Removal/Replacement for information about replacing a power supply.

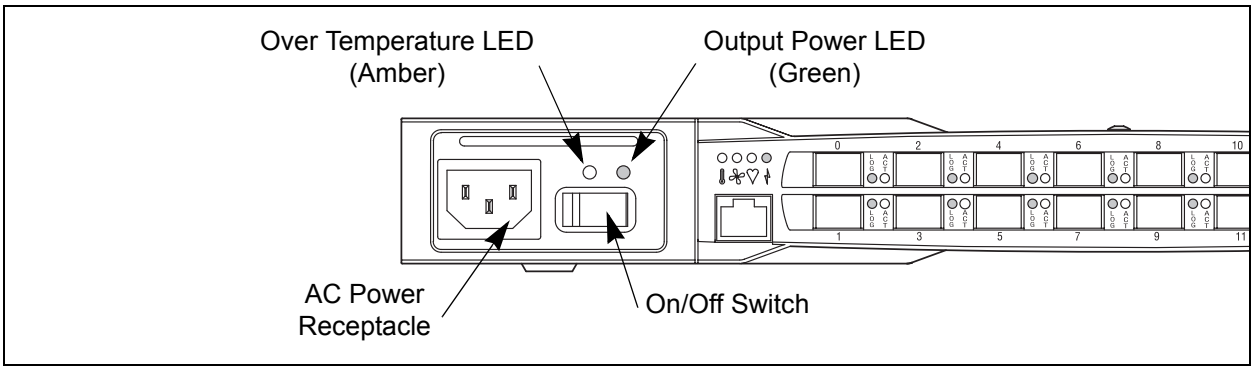


Figure 2-9. Power Supply Components

Each power supply is capable of providing all of the switch's power needs. During normal operation, each power supply provides half of the demand. If one power supply goes offline, the second power supply steps up and provides the difference.

The power supplies are hot swappable and interchangeable. Hot swappable means that you can remove and replace one power supply while the switch is in operation without disrupting service.

Each power supply has two status LEDs: an Output Power LED (green) and an Over Temperature LED (amber):

- The Output Power LED illuminates to indicate that the power supply is producing DC voltage at the proper levels.
- The Over Temperature LED illuminates to indicate that the power supply is overheating. When a power supply overheats, the switch extinguishes the Output Power LED and shuts down the power supply. Refer to Section 5 Diagnostics/Troubleshooting for information about troubleshooting over temperature conditions.

2.7 Fans

The switch is equipped with two fans as shown in Figure 2-10. If one fan should fail, the other fan is capable of providing the necessary cooling until the failed fan can be replaced. The fans are hot swappable and interchangeable. Air flow can be front-to-back or back-to-front depending on the switch model. Refer to "Fans" on page 6-4 for information about removing fans, replacing the fans, and air flow direction.

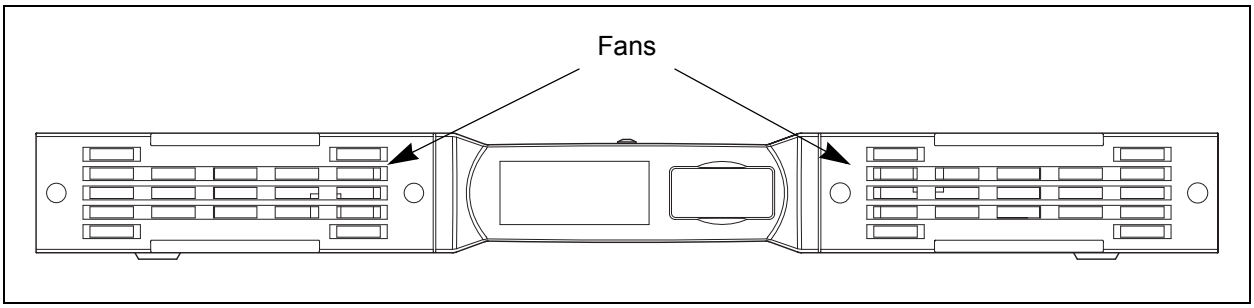


Figure 2-10. Fans

2.8 Switch Management

SANbox Manager is a workstation-based Java® application that provides a graphical user interface for fabric management. This application runs on a Windows®, Solaris™, or Linux® workstation. The management workstation connects to the fabric directly through one switch's Ethernet port and provides in-band management for all other switches in the fabric. Refer to the *SANbox2-8c/16 Switch Management User's Guide* for information about the SANbox Manager application and its use.

In addition to SANbox Manager, the switch supports the following management tools:

- Command Line Interface (CLI)
- File Transfer Protocol (FTP)
- Simple Network Management Protocol (SNMP)

The command line interface provides monitoring and configuration functions by which the administrator can manage the fabric and its switches. The CLI is available over an Ethernet connection or a serial connection. Refer to Appendix B Command Line Interface for more information.

FTP provides the command line interface for exchanging files between the switch and the management workstation. These files include firmware image files, configuration files, and log files.

SNMP provides monitoring and trap functions for the fabric. SANbox2 firmware supports SNMP versions 1 and 2, the Fibre Alliance Management Information Base (FA-MIB) version 4.0, and the Fabric Element Management Information Base (FE-MIB) RFC 2837. Traps can be formatted using SNMP version 1 or 2.

Notes

Section 3
Planning

Consider the following when planning a fabric:

- Devices
- Multiple chassis fabrics
- Performance
- Device access
- Fabric security
- Fabric management

3.1 Devices

When planning a fabric, consider the number of devices and the anticipated demand. This will determine the number of ports that are needed and in turn the number of switches. Consider how many and what types of switches are needed.

The switch uses SFP optical transceivers, but the device host bus adapters you are using may not. Consider whether the device adapters use SFP transceivers or Gigabit Interface Converters (GBIC), and choose fiber optic cable accordingly. Use LC-type cable connectors for SFP transceivers and SC-type cable connectors for GBIC transceivers.

SANbox2 switches support only public devices. Consider the distribution of target and initiator devices. An F_Port supports a single public device. An FL_Port can support up to 126 public devices in an arbitrated loop.

3.2 Multiple Chassis Fabrics

By connecting switches together you can expand the number of available ports for devices. Each switch in the fabric is identified by a unique domain ID, and the fabric will automatically resolve domain ID conflicts. Because the ports are self-configuring, you can connect SANbox2-16 and other FC-SW-2 compliant switches together in a wide variety of topologies.

3.2.1 Domain ID, Principal Priority, and Domain ID Lock

The following switch configuration settings affect multiple chassis fabrics:

- Domain ID
- Principal priority
- Domain ID lock

The domain ID is a unique number from 1–239 that identifies each switch in a fabric. The principal priority is a number (1–255) that determines the principal switch which manages domain ID assignments for the fabric. The switch with the highest principal priority (1 is high, 255 is low) becomes the principal switch. If the principal priority is the same for all switches in a fabric, the switch with the lowest WWN becomes the principal switch.

The domain ID lock allows (False) or prevents (True) the reassignment of the domain ID on that switch. Switches come from the factory with the domain ID set to 1, the domain ID lock set to False, and the principal priority set to 254. Refer to the *SANbox2-8c/16 Switch Management User's Guide* for information about changing the domain ID using SANbox Manager. Refer to the "Set Config Command" on page B-39 for information about changing the default domain ID, domain ID lock, and principal priority parameters.

An unresolved domain ID conflict means that the switch with the higher WWN will isolate as a separate fabric, and the Logged-In LEDs on both switches will flash green to show the affected ports. If you connect a new switch to an existing fabric with its domain ID unlocked, and a domain ID conflict occurs, the new switch will isolate as a separate fabric. However, you can remedy this by resetting the new switch or taking it offline then back online. The principal switch will reassign the domain ID and the switch will join the fabric.

Note: Domain ID reassignment is not reflected in zoning that is defined by domain ID/port number pair or Fibre Channel address. You must reconfigure zones that are affected by domain ID reassignment. To prevent zoning definitions from becoming invalid under these conditions, lock the domain IDs using SANbox Manager or the Set Config Switch command.

3.2.2
Common Topologies

The SANbox2-16 switch supports three commonly used fabric topologies:

- Cascade
- Mesh
- Multistage®

3.2.2.1
Cascade Topology

A cascade topology describes a fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology as shown in Figure 3-1. The loop reduces latency because any switch can route traffic in the shortest direction to any switch in the loop. The loop also provides failover should a switch fail.

The cascade fabric shown in Figure 3-1 has the following characteristics:

- Each chassis link contributes up to 200 MB/s of bandwidth between chassis, 400 MB/s in full duplex. However, because of the sequential structure, that bandwidth will be shared by traffic between devices on other chassis.
- Latency between any two ports is no more than three chassis hops.
- 48 Fibre Channel ports are available for devices.

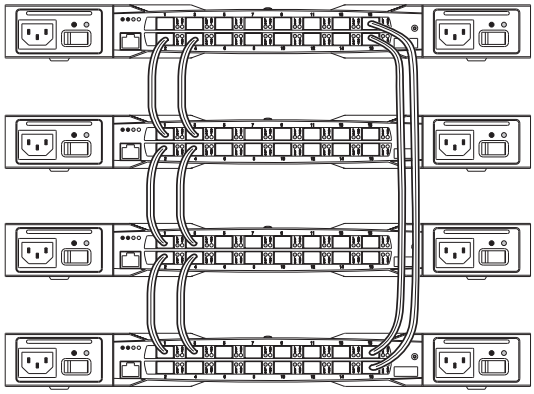


Figure 3-1. Cascade-with-a-Loop Topology

3.2.2.2

Mesh Topology

A mesh topology describes a fabric in which each chassis has at least one port directly connected to each other chassis in the fabric. The example mesh fabric shown in Figure 3-2 has the following characteristics:

- Each link contributes up to 200 MB/s of bandwidth between switches, 400 MB/s in full duplex. Because of multiple parallel paths, there is less competition for this bandwidth than with a cascade or a Multistage topology.
- Latency between any two device ports is no more than two chassis hops.
- 40 Fibre Channel ports are available for devices.

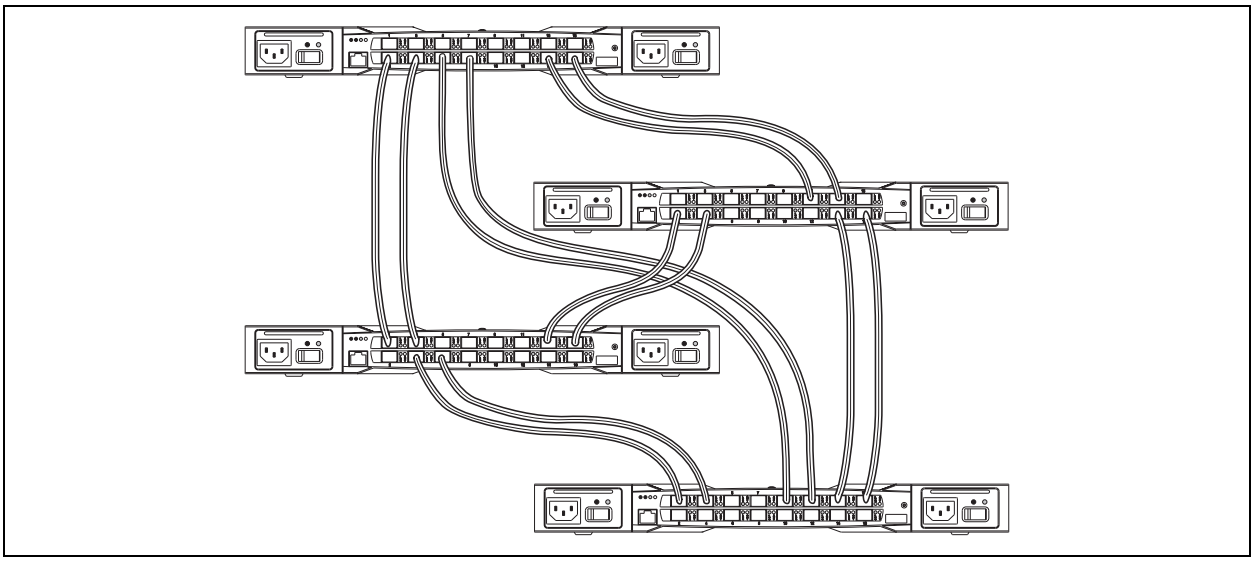


Figure 3-2. Mesh Topology

3.2.2.3

Multistage Topology

A Multistage topology describes a fabric in which two or more edge switches connect to one or more core switches. Each additional core switch increases the bandwidth to each edge switch by 200 MB/s. The Multistage fabric shown in Figure 3-3 has the following characteristics:

- Each link contributes up to 200 MB/s of bandwidth between chassis. Competition for this bandwidth is less than that of a cascade topology, but greater than that of the mesh topology.
- Latency between any two device ports is three chassis hops.
- 52 Fibre Channel ports are available for devices

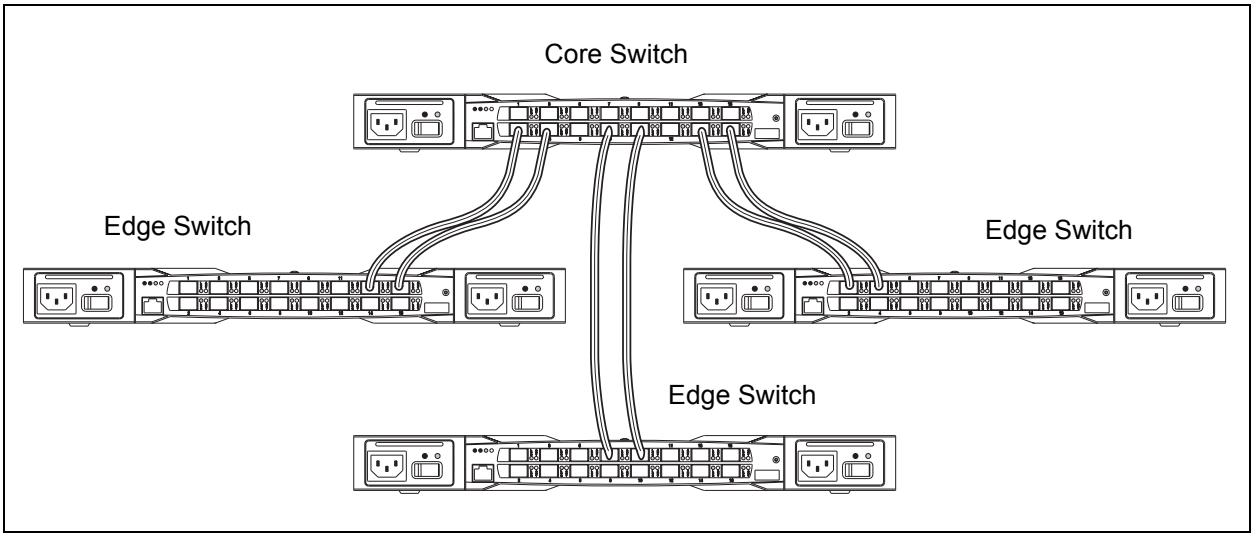


Figure 3-3. Multistage Topology

3.3 Performance

The SANbox2-16 switch supports class 2 and class 3 Fibre Channel service at transmission rates of 1 Gbps or 2 Gbps with a maximum frame size of 2148 bytes. A port can transmit or receive at 1 Gbps or 2 Gbps depending on the device to which it is connected. The port discovers the transmission speed prior to login when the connected device powers up. Related performance characteristics include the following:

- Distance
- Bandwidth
- Latency

3.3.1 Distance

Consider the physical distribution of devices and switches in the fabric. Choose SFP transceivers that are compatible with the cable type, distance, Fibre Channel revision level, and the device host bus adapter. Refer to Appendix A Specifications for more information about cable types and SFP transceivers.

Each port is supported by a data buffer with a 12 credit capacity; that is, 12 maximum sized frames. For fibre optic cables, this enables full bandwidth over a distance of 20 kilometers at 1 Gbps (0.6 credits/Km), or 10 kilometers at 2 Gbps (1.2 credits/Km). Beyond this distance, however, there is some loss of efficiency because the transmitting port must wait for an acknowledgement before sending the next frame.

Longer distances can be spanned at full bandwidth by extending credits on G_Ports and F_Ports. Each port can donate up to 11 credits to a pool from which a recipient port can borrow. For example, you can configure a recipient port to borrow up to 66 credits from 6 ports for a total of 78 credits. This will support communication over approximately 130 Km at 1 Gbps (78÷0.6) or 65 Km at 2 Gbps (78÷1.2).

You can configure recipient and donor ports using SANbox Manager or the Set Config command. Refer to ”Set Config Command” on page B-39 for more information.

3.3.2 Bandwidth

Bandwidth is a measure of the volume of data that can be transmitted at a given transmission rate. A port can transmit or receive at 1 Gbps or 2 Gbps depending on the device to which it is connected. The switch supports all transmission rate combinations as shown in Table 3-1.

Table 3-1. Port-to-Port Transmission Combinations

Source Port Rate	Destination Port Rate	Maximum Bandwdith
1 Gbps	1 Gbps	100 MB
1 Gbps	2 Gbps	100 MB
1 Gbps x 2 ports	2 Gbps	200 MB
2 Gbps	1 Gbps x 2 ports	100 MB each port[1]
2 Gbps	2 Gbps	200 MB

[1]Bandwidth will be less for larger sequence sizes.

In multiple chassis fabrics, each link between chassis contributes 100 or 200 megabytes of bandwidth between those chassis. When additional bandwidth is needed between devices, increase the number of links between the connecting switches. The switch guarantees in-order-delivery with any number of links between chassis.

3.3.3 Latency

Latency is a measure of how fast a frame travels from one port to another. The factors that affect latency include transmission rate and the source/destination port relationship as shown in Table 3-2.

Table 3-2. Port-to-Port Latency

Source/Destination Rates	Same Switch I
1 Gbps - 1 Gbps	< 1 µsec
2 Gbps - 2 Gbps	< 0.4 µsec

3.4 Device Access

Consider device access needs within the fabric. Access is controlled by the use of zones and zone sets. Some zoning strategies include the following:

- Separate devices that use different operating systems.
- Separate devices that have no need to communicate with other devices in the fabric or have classified data.
- Separate devices into department, administrative, or other functional group.
- Reserve a path and its bandwidth from one port to another.

A zone is a named group of devices that can communicate with each other. Membership in a zone can be defined by switch port number, port Fibre Channel address, or by device worldwide name (WWN). Devices can communicate only with devices that are members of the same zone. A zone can be a member of more than one zone set. Several zone sets can be defined for a fabric, but only one zone set can be active at one time. The active zone set determines the current fabric zoning.

A zoning database is maintained on each switch consisting of all inactive zone sets, the active zone set, all zones, aliases, and their membership. The switch supports the following maximum limits:

- 256 zone sets
- 256 zones per zone set
- 1000 total zones
- 2000 members per zone
- 256 aliases
- 2000 members per alias
- 2000 total number of alias and zone members

The following zone types are supported:

- Soft zone
- Access Control List (ACL) - hard zone
- Virtual Private Fabric (VPF) - hard zone

3.4.1
Soft Zones

Soft zoning divides the fabric for purposes of controlling discovery. Members of the same soft zone automatically discover and communicate freely with all other members of the same zone. The soft zone boundary is not secure; traffic across soft zones can occur if addressed correctly. The following rules apply to soft zones:

- Soft zones that include members from multiple switches need not include the ports of the inter-switch links.
- Soft zone boundaries yield to ACL and VPF zone boundaries.
- Soft zones can overlap; that is, a port can be a member of more than one soft zone.
- Membership can be defined by Fibre Channel address, domain ID and port number, or worldwide name.
- Soft zoning supports all port modes.

3.4.2
Access Control List Hard Zones

Access Control List (ACL) zoning divides the fabric for purposes of controlling discovery and inbound traffic. ACL zoning is a type of hard zoning that is hardware enforced. This type of zoning is useful for controlling access to certain devices without totally isolating them from the fabric. Members can communicate with each other and transmit outside the ACL zone, but cannot receive inbound traffic from outside the zone. The following rules apply to ACL zones:

- The ACL zone boundary is secure against inbound traffic.
- ACL zones can overlap; that is, a port can be a member of more than one ACL zone.
- ACL zones that include members from multiple switches need not include the ports of the inter-switch links.
- ACL zone boundaries supersede soft zone boundaries, but yield to VPF zone boundaries.
- Membership can be defined only by domain ID and port ID.
- ACL zoning supports all port modes.

3.4.3
Virtual Private Fabric Hard Zones

Virtual Private Fabric (VPF) zoning divides the fabric for purposes of controlling discovery and both inbound and outbound traffic. This type of zoning is useful for providing security and reserving paths between devices to guarantee bandwidth. VPF zoning is a type of hard zoning that is hardware enforced. Members can only transmit to and receive from members of the same VPF zone. The VPF zone boundary is secure against both inbound and outbound traffic. The following rules apply to VPF zones:

- VPF zones that include members from multiple switches must include the ports of the inter-switch links.
- VPF zones cannot overlap; that is, a port can be a member of only one VPF zone.
- VPF zone boundaries supersede both soft and ACL zone boundaries.
- Membership can be defined only by domain ID and port ID.
- VPF zoning supports all port modes.

Fabric Security

An effective security profile begins with a security policy that states the requirements. A threat analysis is needed to define the plan of action followed by an implementation that meets the security policy requirements. Internet portals, such as remote access and email, usually present the greatest threats. Fabric security should also be considered in defining the IT infrastructure security policy.

Most fabrics are located at a single site and are protected by physical security, such as key-code locked computer rooms. For these cases, security methods such as user passwords for equipment and zoning for controlling device access, are satisfactory.

Fabric security is needed when security policy requirements are more demanding: for example, when fabrics span multiple locations and traditional physical protection is insufficient to protect the IT infrastructure. Another benefit of fabric security is that it creates a structure that helps prevent unintended changes to the fabric.

Fabric security consists of the following:

- User account security
- Device security
- Fabric services

3.4.4
User Account Security

User account security consists of the administration of account names, passwords, expiration date, and authority level. If an account has Admin authority, all management tasks can be performed by that account in both SANbox Manager and the Command Line Interface. Otherwise only monitoring tasks are available. The default account name, Admin, is the only account that can administer user accounts. Refer to ”Device Security” on page 3-11. Consider your management needs and determine the number of user accounts, their authority needs, and expiration dates.

Account names and passwords are always required when connecting to a switch through Telnet. However, SANbox Manager does not authenticate account names when opening a fabric unless the UserAuthentication parameter is set to True using the Set Setup System command. Refer to the ”Set Setup Command” on page B-54 for more information. The UserAuthentication parameter must be configured the same for all switches in the fabric. If the UserAuthentication parameter is False (default), SANbox Manager logs you in with the Admin account name and password (password). Consider your user accounts and determine whether user authentication is necessary.

3.4.5
Device Security

Device security provides for the authorization and authentication of devices that you attach to a switch. You can configure a switch with a group of devices against which the switch authorizes new attachments by devices, other switches, or applications issuing management server commands. In addition to authorization, the switch can be configured to require authentication of the connecting device through the use of a password or secret.

Device security is configured through the use of security sets and groups. A group is a list of device worldwide names that are authorized to attach to a switch. There are three types of groups: one for other switches (ISL), another for N_Port devices (port), and a third for devices or applications issuing management server commands (MS). Device security is not supported for loop devices. A security set is a set of up to three groups with no more than one of each group type. The security database is made up of all security sets on the switch. The security database has the following limits:

- The maximum number of security sets is 4.
- The maximum number of groups is 16.
- The maximum number of members in a group is 1000.
- The maximum total number of group members is 1000.

Consider the devices, switches, and management agents and evaluate the need for authorization and authentication.

The following examples illustrate how to configure a security database.

3.4.5.1

Security Example: Switches and HBAs

Consider the fabric shown in Figure 3-4. In this fabric, Switch_1 and HBA_1 support security while the JBOD, Switch_2 and HBA_2 do not. The objective is to secure F_Ports and E_Ports in the fabric. To do this, configure security on the devices that support security: Switch_1 and HBA_1.

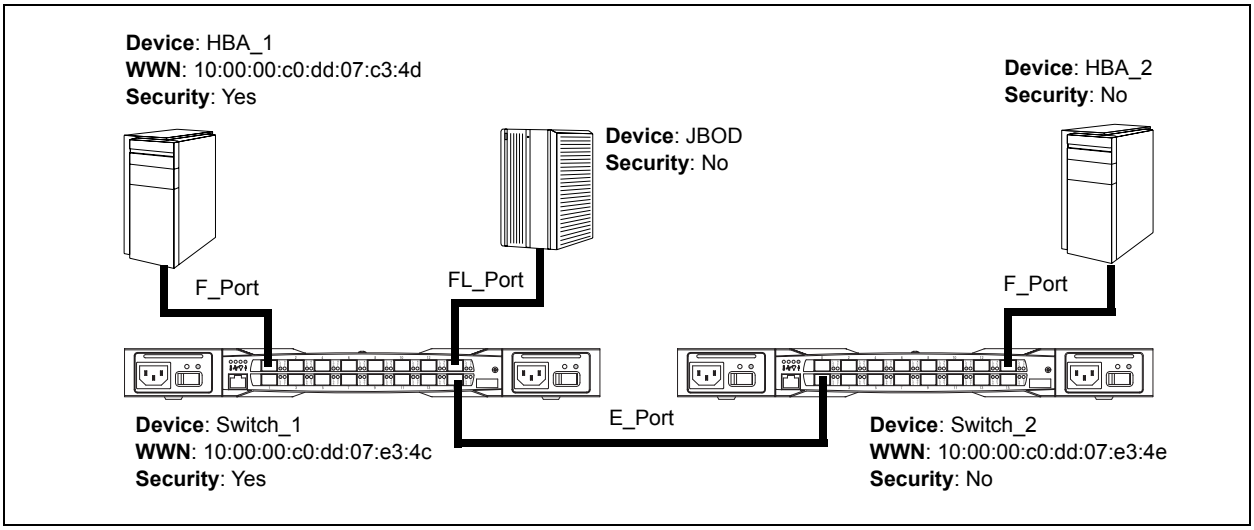


Figure 3-4. Security Example: Switches and HBAs

1. Create a security set (Security_Set_1) on Switch_1.
2. Create a port group (Group_Port) in Security_Set_1 with Switch_1, and HBA_1 as members. Because the JBOD is a loop device, it is excluded from the port group.
   - You must specify HBAs by node worldwide name. Switches can be specified by port or node worldwide name. The type of switch worldwide name you use in the switch security database must be the same as that in the HBA security database. For example, if you specify a switch with a port worldwide name in the switch security database, you must also specify that switch in the HBA security database with the same port worldwide name.
   - For CHAP authentication, create 32-character secrets. The switch secret must be shared with the HBA security database.

Port Group: Group_Port	
Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Secret: 0123456789abcdef0123456789abcdef
HBA_1	Node WWN: 10:00:00:c0:dd:07:c3:4d Authentication: CHAP Secret: fedcba9876543210fedcba9876543210fedcba

3. Create an ISL group (Group_ISL) in Security_Set_1 with Switch_2 as its member. Only Switch_2 need be a member because there is no authentication between the switches.

ISL Group: Group_ISL	
Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: None Binding: None

4. Configure security on HBA_1 using the appropriate management tool. Logins between the Switch_1 and HBA_1 will be challenged (CHAP) for their respective secrets. Therefore, the secrets for Switch_1 and HBA_1 that you configured on Switch_1 must also be configured on HBA_1.
5. Save Security_Set_1 and prepare to activate it. Activating a security set does not affect currently logged-in ports. Therefore, to apply the security policy that you designed in the security database, you must offline the secured ports, activate the security set, then place the secured ports back online.

3.4.5.2
Security Example: Host Authentication

Consider the fabric shown in Figure 3-5. In this fabric, only Switch_2 and HBA_2/APP_2 support security, where APP_2 is a host application. The objective is to secure the management server on Switch_2 from unauthorized access by an HBA or an associated host application.

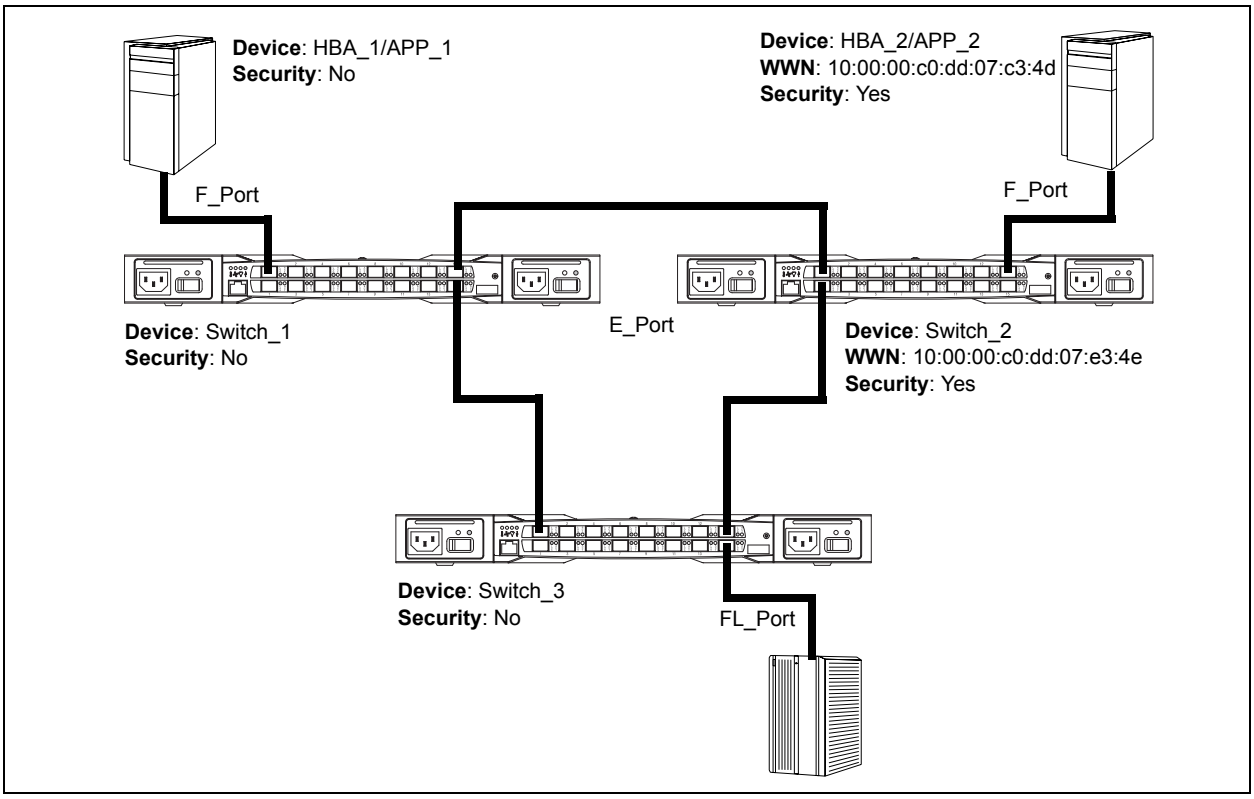


Figure 3-5. Security Example: Management Server

1. Create a security set (Security_Set_2) on Switch_2.
2. Create a Management Server group (Group_1) in Security_Set_2 with Switch_2 and HBA_2 or APP_2 as its member.
   - You must specify HBAs by node worldwide name. Switches can be specified by port or node worldwide name. The type of switch worldwide name you use in the switch security database must be the same as that in the HBA security database. For example, if you specify a switch with a port worldwide name in the switch security database, you must also specify that switch in the HBA security database with the same port worldwide name.
   - For MD5 authentication, create 32-character hex secrets.

MS Group: Group_1	
Switch_2	Node WWN: 10:00:00:c0:dd:07:c3:4e CT Authentication: MD5 Secret: 9876543210fedcba9876543210fedcba
HBA_2 or APP_2	Node WWN: 10:00:00:c0:dd:07:c3:4d CT Authentication: MD5 Secret: fedcba9876543210fedcba9876543210

3. Configure security on HBA_2 or APP_2 using the appropriate management tool. Logins between the Switch_2 and HBA_2 or APP_2 will be challenged (MD5) for their respective secrets. Therefore, the secrets that you configured for HBA_2 or APP_2 on Switch_2 must also be configured on HBA_2 or APP_2.
4. Save Security_Set_2 and prepare to activate it. Activating a security set does not affect currently logged-in ports. Therefore, to apply the security policy that you designed in the security database, you must offline the secured ports, activate the security set, then place the secured ports back online.

3.4.6 Fabric Services

Fabric services include security-related functions such as inband management and SNMP. Inband management is the ability to manage switches across inter-switch links using SANbox Manager, SNMP, management server, or the application programming interface. The switch comes from the factory with inband management enabled. If you disable inband management on a particular switch, you can no longer communicate with that switch by means other than a direct Ethernet or serial connection. You can also enable or disable SNMP. Consider how you want to manage the fabric and what switches you do not want managed through another switch.

3.5

Fabric Management

The SANbox Manager application and CLI execute on a management workstation that provides for the configuration, control, and maintenance of the fabric. Supported platforms include Windows, Windows NT, Solaris, and Linux. The SANbox Manager application can manage multiple fabrics. Consider how many fabrics will be managed, how many management workstations are needed, and whether the fabrics will be managed with the CLI or SANbox Manager.

A switch supports a combined maximum of 19 logins reserved as follows:

- 4 sessions for internal applications such as management server and SNMP
- 15 sessions for SANbox Manager inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins and Telnet logins. Of these 15, there can be a combined maximum of 10 SANbox Manager and API logins. Additional logins will be refused.

Section 4

Installation

This section describes how to install and configure the SANbox2-16 switch. It also describes how to load new firmware and how to recover a disabled switch.

4.1 Site Requirements

Consider the following items when installing a SANbox2-16 switch:

- Fabric management workstation
- Power requirements
- Environmental conditions

4.1.1 Fabric Management Workstation

The requirements for fabric management workstations running SANbox Manager are described in Table 4-1:

Table 4-1. Management Workstation Requirements

Operating System	■ Windows® NT, 2000, 95/98 ■ Linux® 7.2 Red Hat® ■ Solaris™
Memory	128 MB or more
Disk Space	150 MB per installation
Processor	300 MHz or faster
Hardware	CD-ROM drive, RS-232 serial port, RJ-45 Ethernet port
Internet Browser	Microsoft® Internet Explorer® or Netscape Navigator®

Telnet workstations require an RJ-45 Ethernet port or an RS-232 serial port and an operating system with a Telnet client.

4.1.2 Switch Power Requirements

Operating voltage requirements are as follows:

90 to 137 VAC; 47 to 63 Hz
180 to 265 VAC; 47 to 63 Hz

4.1.3 Environmental Conditions

Consider the factors that affect the climate in your facility such as equipment heat dissipation and ventilation. The switch requires the following operating conditions:

- Operating temperature range: 10° – 40° C (50°– 104°F)
- Relative humidity: 25 – 80%, non-condensing

4.2 Installing a Switch

Unpack the switch and accessories. The SANbox2-16 product is shipped with the components shown in Figure 4-1:

- SANbox2-16 Fibre Channel Switch (1) with firmware installed
- Power cords (2)
- Rubber feet (4)
- Rack mount brackets (2)
- CD-ROM containing the SANbox Manager switch management application, release notes, and documentation.

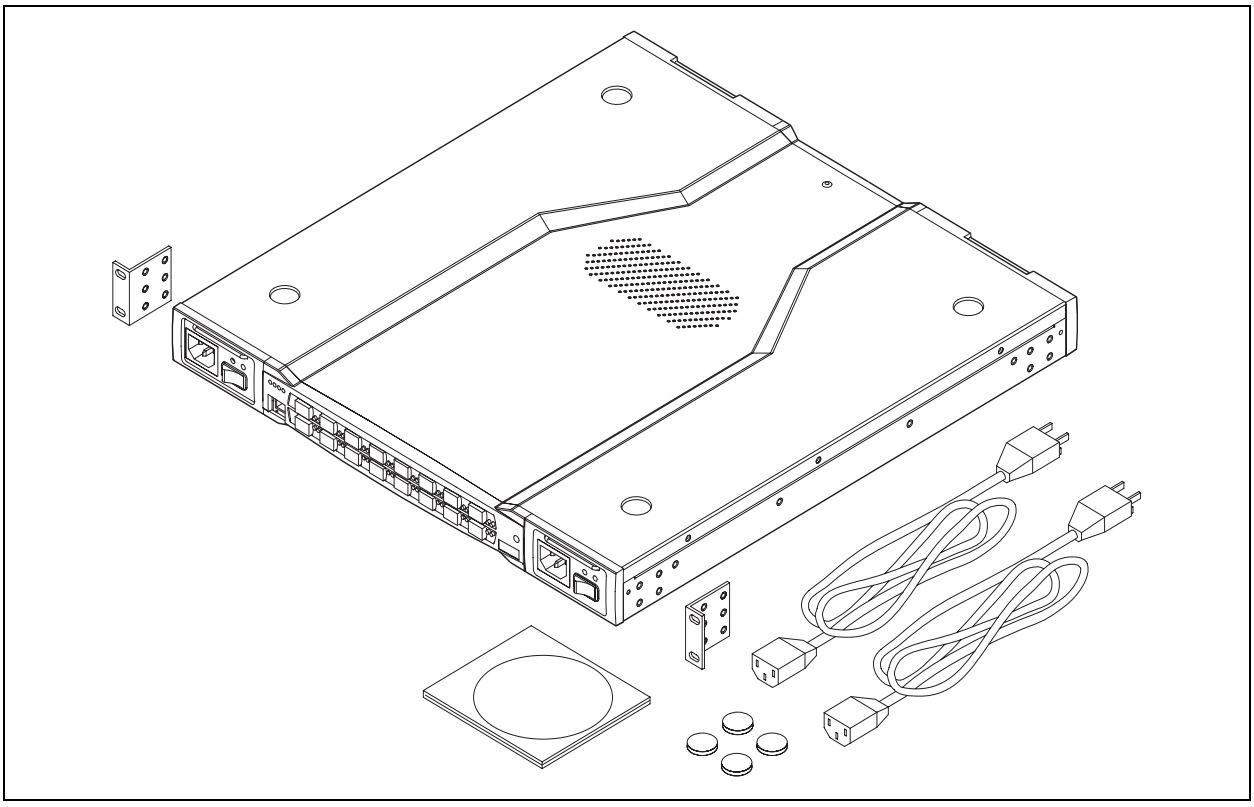


Figure 4-1. SANbox2-16 Fibre Channel Switch

Installing a SANbox2-16 switch involves the following steps:

1. Mount the switch.
2. Install SFP transceivers.
3. Connect the switch to the AC power source.
4. Connect the management workstation to the switch.
5. Install the SANbox Manager application.
6. Configure the switch.
7. Configure the ports.
8. Cable devices to the switch.

4.2.1 Mount the Switch

The switch can be placed on a flat surface and stacked or mounted in a 19” EIA rack. The top of each chassis has dimples to receive the rubber feet of a second chassis stacked on top. Without the rubber feet, the switch occupies 1U of space in an EIA rack. Mounting rails are required for rack installation and are available through QLogic Corporation.

WARNING!! Mount switches in the rack so that the weight is distributed evenly. An unevenly loaded rack can become unstable possibly resulting in equipment damage or personal injury.

AVERTISSEMENT!!

Installer les commutateurs dans l’armoire informatique de sorte que le poids soit réparti uniformément. Une armoire informatique déséquilibré risque d'entraîner des blessures ou d'endommager l'équipement.

WARNUNG!!

Switches so in das Rack einbauen, dass das Gewicht gleichmäßig verteilt ist. Ein Rack mit ungleichmäßiger Gewichtsverteilung kann schwanken/umfallen und Gerätbeschädigung oder Verletzung verursachen.

CAUTION!

- If the switch is mounted in a closed or multi-unit rack assembly, make sure that the operating temperature inside the rack enclosure does not exceed the maximum rated ambient temperature. Refer to ”Environmental” on page A-4.
- The switch must rest on rails or a shelf in the rack or cabinet. Allow 16 cm (6.5 in) minimum clearance at the front and rear of the rack for service access and ventilation.
- Do not restrict chassis air flow. Allow 16 cm (6.5 in) minimum clearance at the front and rear of the rack for service access and ventilation.
- Multiple rack-mounted units connected to the AC supply circuit may overload that circuit or overload the AC supply wiring. Consider the power source capacity and the total power usage of all switches on the circuit. Refer to ”Electrical” on page A-3.
- Reliable grounding in the rack must be maintained from the switch chassis to the AC power source.

When mounting the switch in a rack, ensure that the 19-inch rack meets the following standard specifications:

- ANSI/EIA RS-230 Standard, entitled *Cabinets, Racks, Panels, and Associated Equipment*
- MIL-STD- 189, entitled *Racks, Electrical Equipment, 19-Inch and Associated Panels*

The brackets shown in Figure 4-2 are provided with the switch so that the switch can be secured on a shelf. The brackets alone are not designed to support the weight of the switch.

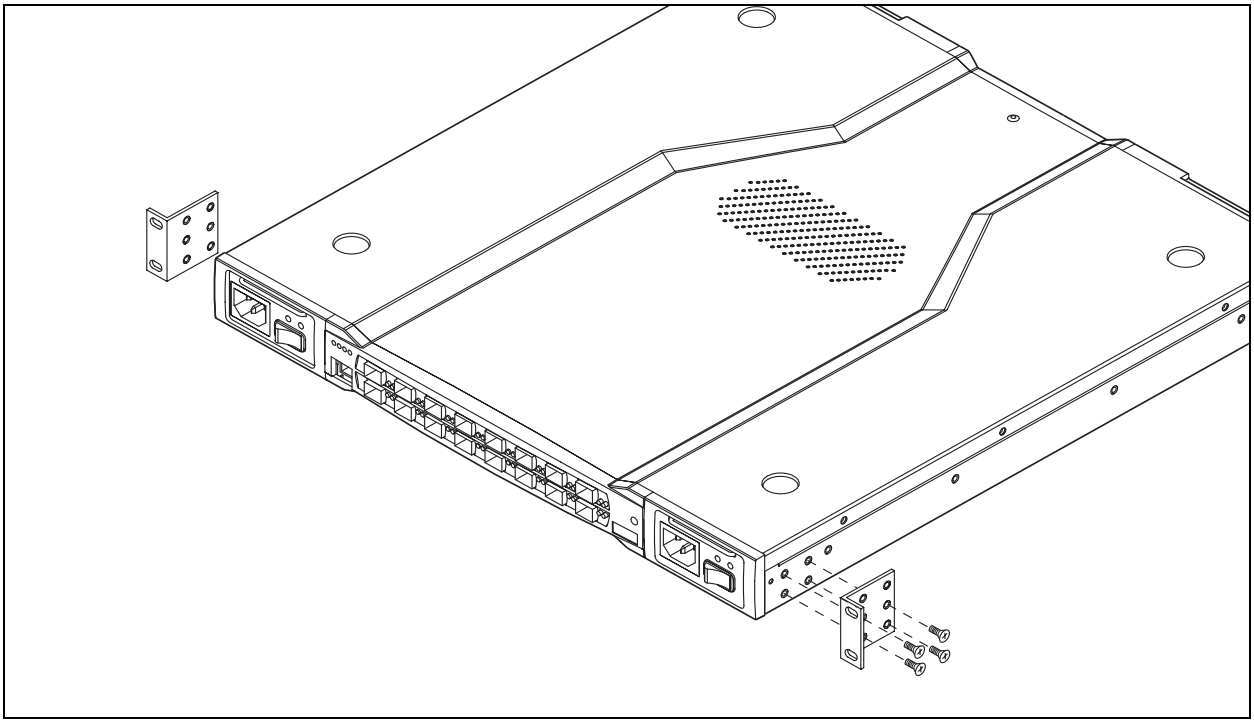


Figure 4-2. Installing Rack Mount Brackets

4.2.2
Install SFP Transceivers

The switch has been validated with transceivers that support a variety of interconnection media. To install, insert the transceiver into the port and gently press until it snaps in place. To remove a transceiver, gently press the transceiver into the port to release the tension, then pull on the release tab or lever and remove the transceiver. Different transceiver manufacturers have different release mechanisms. Consult the documentation for your transceiver.

Note: The SFP transceiver will fit only one way. If the SFP does not install under gentle pressure, flip it over and try again.

4.2.3
Connect the Switch to AC Power

WARNING!! This product is supplied with a 3-wire power cable and plug for the user's safety. Use this power cable in conjunction with a properly grounded outlet to avoid electrical shock. An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the switch chassis. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent electrical shock.

You may require a different power cable in some countries because the plug on the cable supplied with the equipment will not fit your electrical outlet. In this case, you must supply your own power cable. The cable you use must meet the following requirements:

- For 125 Volt electrical service, the cable must be rated at 10 Amps and be approved by UL and CSA.
- For 250 Volt electrical service: The cable must be rated at 10 Amps, meet the requirements of H05VV-F, and be approved by VDE, SEMKO, and DEMKO.

AVERTISSEMENT!!

Pour la sécurité de l'utilisateur, l'appareil est livré avec un câble d'alimentation trifilaire et une fiche. Pour éviter toute secousse électrique, enficher ce câble à une prise correctement mise à la terre.Une prise électrique dont les fils sont mal branchés peut créer une tension dangereuse dans les pièces métalliques du châssis switch. Pour éviter toute secousse électrique, s'assurer que les fils sont correctement branchés et que la prise est bien mise à la terre.

Dans certains pays les prises électriques sont de modèle différent; on ne peut y enficher le câble de l'appareil. On doit donc en utiliser un autre ayant les caractéristiques suivantes:

- Alimentation 125 V: Câble pour courant nominal de 10 A, agréé LAC et CSA.
- Alimentation 250 V: Câble pour courant nominal de 10 A, conforme au H05VV-F, et agréé VDE, SEMKO et DEMKO.

WARNUNG!!

Dieses Produkt wird mit einem 3-adrigen Netzkabel mit Stecker geliefert. Dieses Kabel erfüllt die Sicherheitsanforderungen und sollte an einer vorschriftsmäßigen Schukosteckdose angeschlossen werden, um die Gefahr eines elektrischen Schlages zu vermeiden.Elektrosteckdosen, die nicht richtig verdrahtet sind, können gefährliche Hochspannung an den Metallteilen des switch-Gehäuses verursachen. Der Kunde trägt die Verantwortung für eine vorschriftsmäßige Verdrahtung und Erdung der Steckdose zur Vermeidung eines elektrischen Schlages.

In manchen Ländern ist eventuell die Verwendung eines anderen Kabels erforderlich, da der Stecker des mitgelieferten Kabels nicht in die landesüblichen Steckdosen paßt. In diesem Fall müssen Sie sich ein Kabel besorgen, daß die folgenden Anforderungen erfüllt:

- Für 125 Volt-Netze: 10 Ampere Kabel mit UL- und CSA-Zulassung.
- Für 250 Volt-Netze: 10 Ampere Kabel gemäß den Anforderungen der H05VV-F und VDE-, SEMKO- und DEMKO-Zulassung.

To energize the switch, do the following:

1. Connect the power cords to the AC power receptacles on the front of the switch chassis.
2. Connect each power cord to a 3-wire, grounded, AC outlet that delivers power in accordance with the power requirements in Appendix A Specifications.

Note: To provide redundancy in the event of an AC power circuit failure, connect the switch power supplies to separate AC circuits.

3. Place one or both power On/Off switches in the On position to energize the switch logic circuitry. Confirm that the Input Power LED on the switch chassis is illuminated indicating that the switch logic circuitry is receiving DC voltage. If not, contact your authorized maintenance provider.

4. Confirm that the Output Power LEDs on both power supplies are illuminated. If not, do the following:
   a. Check voltage at the AC power source.
   b. Inspect the power cord.
   c. Replace the power supply.
5. Observe the Heartbeat LED to determine the results of the Power On Self Test (POST). The POST tests the condition of firmware, memories, data-paths, and switch logic circuitry and passes a blink code to the Heartbeat LED. If the Heartbeat LED blinks steadily about once per second, the POST was successful, and you can continue with the installation process. Any other blink pattern appears indicates that an error has occurred. Refer to ”Heartbeat LED Blink Patterns” on page 5-1 for more information about the error blink pattern.

4.2.4
Connect the Management Workstation to the Switch

Connect the management workstation to the switch in one of three ways:

- Indirect Ethernet connection from the management workstation to the switch RJ-45 Ethernet connector through an Ethernet switch or a hub. This requires a 10/100 Base-T straight cable as shown in Figure 4-3. With this method, you can manage the switch with the SANbox Manager application or Command Line Interface.
- Direct Ethernet connection from the management workstation to the switch RJ-45 Ethernet connector. This requires a 10/100 Base-T cross-over cable as shown in Figure 4-3. With this method, you can manage the switch with the SANbox Manager application or Command Line Interface.
- Serial port connection from the management workstation to the switch RS-232 serial port connector. This requires a null modem F/F DB9 cable as shown in Figure 4-3. With this method, you can manage the switch with Command Line Interface.

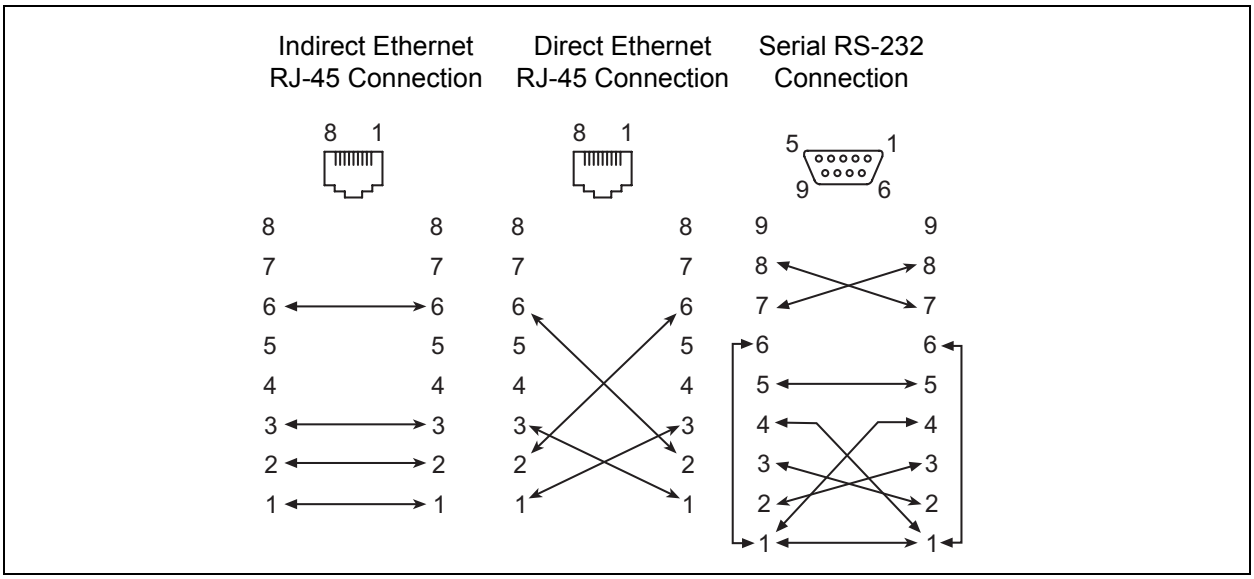

Indirect Ethernet
RJ-45 Connection
Direct Ethernet
RJ-45 Connection
Serial RS-232
Connection
8 1
8 1
5 1
9 6
8 7 6 5 4 3 2 1
8 7 6 5 4 3 2 1
8 7 6 5 4 3 2 1
8 7 6 5 4 3 2 1
9 8 7 6 5 4 3 2 1
9 8 7 6 5 4 3 2 1

Figure 4-3. Ethernet and Serial Cable Connections

4.2.4.1
Ethernet Connection

To establish an Ethernet connection, do the following:

1. Connect a 10/100 Base-T cross-over cable from an RJ-45 port on the management workstation directly to the RJ-45 Ethernet port; or a 10/100 Base-T straight cable indirectly over an Ethernet network.
2. Open a Telnet session by entering the following command with the switch IP address. The default IP address is 10.0.0.1

```
telnet 10.0.0.1
```

3. Log in to the switch. If user authentication is disabled, account names and passwords are not enforced. Refer to the ”Set Setup Command” on page B-54 for information about setting fabric security. The default account name and password are (admin, password).

```
SANbox2 Login: admin
Password: ********
```

4.2.4.2
Serial Connection

To establish a serial port connection, do the following:

1. Connect a null modem F/F DB9 cable from a COM port on the management workstation to the RS-232 serial port on the switch.
2. Configure the connection according to your platform:
   - For Windows:
     a. Open the HyperTerminal application on a Windows platform. Choose the **Start** button, select **Programs, Accessories, HyperTerminal,** and **HyperTerminal**.
     b. Enter a name for the switch connection and choose an icon in the Connection Description window. Choose the **OK** button.
     c. Select the COM port in the Connect To window and choose the **OK** button.
     d. Enter the following COM Port settings in the COM Properties window and choose the **OK** button.
        - q Bits per second: 9600
        - q Data Bits: 8
        - q Parity: None
        - q Stop Bits: 1
        - q Flow Control: None

- For Linux:
  a. Set up minicom to use the serial port. Create or modify the /etc/minirc.dfl file with the following content:

```
pr portdev/ttyS0
pu minit
pu mreset
pu mhangup
```

  b. Verify that all users have permission to run minicom. Review the /etc/minicom/users file and confirm that the line "ALL" exists or that there are specific user entries.

  c. Enter the following command at the Linux prompt:

```
minicom
```

- For Solaris:
  a. Set up Solaris to use the serial port. Modify the /etc/remote file to include the following lines:

```
sanbox2:\
:dv=/dev/term/a:br#9600:el=C^S^Q^U^D:ie%$:oe=^D:
```

  b. Enter the following command at the Solaris prompt:

```
# tip sanbox2
```

3. Log in to the switch. If user authentication is disabled, account names and passwords are not enforced. Refer to the "Set Setup Command" on page B-54 for information about setting user authentication. The default account name and password are (admin, password).

```
SANbox2 Login: admin
Password: ********
```

4.2.5 Install SANbox Manager

You can install SANbox Manager on the Windows, Linux, and Solaris platforms. Your switch was shipped with either a SANsurfer® Management Suite Disk or a SANbox2 Installation Disk. Refer to the following installation instructions that correspond to your situation:

- SANsurfer Management Suite Disk - Windows Installation
- SANsurfer Management Suite Disk - Linux Installation
- SANsurfer Management Suite Disk - Solaris Installation
- SANbox2 Installation Disk - Windows Installation
- SANbox2 Installation Disk - Linux Installation
- SANbox2 Installation Disk - Solaris Installation

4.2.6
SANsurfer Management Suite Disk - Windows Installation

To install the SANbox Manager application on Windows from the SANsurfer® Management Suite Disk, do the following:

1. Close all programs currently running, and insert the SANsurfer Management Suite Disk into the management workstation CD-ROM drive. If the SANsurfer Management Suite start page does not open in your default browser, do the following:
    a. Using Windows Explorer, double-click the drive letter which contains the SANsurfer Management Suite Disk.
    b. Locate and double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page in your default browser.
2. On the SANsurfer Management Suite start page, choose the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 (2Gb) Series area.
4. In the Windows column, choose the **SANbox Manager** link to open the File Download window.
5. You have a choice of running the installation file from the CD-ROM or downloading the installation file to your hard drive. Choose one of the following:
    - Open the installation file from the CD-ROM and follow the SANbox Manager installation instructions.
    - Specify a location in which to save the **sansurfer_windows_install.exe** file, and choose the **Save** button. Double-click the saved **sansurfer_windows_install.exe** file and follow the SANbox Manager installation instructions.

4.2.7
SANsurfer Management Suite Disk - Linux Installation

To install the SANbox Manager application on Linux from the SANsurfer Management Suite Disk, do the following:

1. Close all programs currently running, and insert the SANsurfer Management Suite Disk into the management workstation CD-ROM drive. If a file browser window opens showing icons for the contents of the CD-ROM, double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page. If a file browser does not open, double-click the CD-ROM icon on the to open the browser. If there is no CD-ROM icon, do the following:
    a. Open an xterm or other terminal window.

b. Mount the CD-ROM. From a shell prompt, enter the following command:

```
mount /mnt/cdrom
```

c. Execute your web browser to view the **Start_Here.htm** document using one of the following commands:

```
$mozilla file:/mnt/cdrom/Start_Here.htm
```

or

```
$netscape file:/mnt/cdrom/Start_Here.htm
```

d. The SANsurfer Management Suite start page opens in your default browser.

2. On the SANsurfer Management Suite start page, choose the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 (2Gb) Series area.
4. In the Linux column, choose the **SANbox Manager** link to open the Save As window.
5. Enter a path name to save the **sansurfer_linux_install.bin** file, and choose the **Save** button.
6. Open a terminal window for the directory in which the **sansurfer_linux_install.bin** file was saved, and enter the following command and press the **Enter** key:

```
chmod +x sansurfer_linux_install.bin
```

7. Enter the following command:

```
./sansurfer_linux_install.bin
```

8. Press the **Enter** key, and follow the SANbox Manager installation instructions.

4.2.8 SANsurfer Management Suite Disk - Solaris Installation

To install the SANbox Manager application on Solaris from the SANsurfer Management Suite CD-ROM, do the following:

1. Close all programs currently running, and insert the SANsurfer Management Suite Disk into the management workstation CD-ROM drive. If the SANsurfer Management Suite start page does not open in your default browser, do the following:
   a. Right-click the to open the Workshops Menu.
   b. Point to and select **Files**, then select **File Manager**.

c. In File Manager, double-click the CD-ROM icon, and then double-click the Sansurfer folder.

d. In the Sansurfer folder, double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page in your default browser.

2. On the SANsurfer Management Suite start page, choose the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 (2Gb) Series area.
4. In the Solaris column, choose the **SANbox Manager** link to open the Save As window.
5. Enter a path name to save the **sansurfer_solaris_install.pkg** file and choose the **Save** button.
6. Open a terminal window for the directory in which the **sansurfer_solaris_install.pkg** file was saved, and enter the following command:

```
chmod +x sansurfer_solaris_install.pkg
```

7. Enter the following command and follow the SANbox Manager installation instructions:

```
pkgadd -d QLGCsol_x.x.yyyy.mm.dd.xx.xx
```

Note: If you download SANbox Manager from a server, be sure the downloaded file has execute permission before installing.

4.2.9 SANbox2 Installation Disk - Windows Installation

To install the SANbox Manager application on Windows from the SANbox2 Installation Disk, do the following:

1. Close all programs currently running, and insert the SANbox2 Installation Disk into the management workstation CD-ROM drive.
2. Using Windows Explorer, double-click the drive letter which contains the SANbox2 Installation Disk.
3. Double click the SANbox_Manager folder, then double click the Windows folder.
4. Double click the executable file and follow the SANbox Manager installation instructions.

4.2.10
SANbox2 Installation Disk - Linux Installation

To install the SANbox Manager application on Linux from the SANbox2 Installation Disk, do the following:

1. Close all programs currently running, and insert the SANbox2 Installation Disk into the management workstation CD-ROM drive.
2. Open the File Manager and double-click on the CD-ROM icon.
3. Double click the SANbox_Manager folder, then double click the Linux folder.
4. Double click the executable file and follow the SANbox Manager installation instructions.

4.2.10.1
SANbox2 Installation Disk - Solaris Installation

To install the SANbox Manager application on Solaris from the SANbox2 Installation Disk, do the following:

1. Close all programs currently running, and insert the SANbox2 Installation Disk into the management workstation CD-ROM drive.
2. Open a terminal window. If the disk isn't already mounted, enter the following command:

   ```
   mount /mnt/cdrom
   ```

3. Move the directory on the disk that contains the executable. Enter the following command:

   ```
   cd cdrom/cdrom0/sanbox~1/solaris
   ```

4. Run the executable and follow the SANbox Manager installation instructions. Enter the following command:

   ```
   pkgadd -d sol_pkg
   ```

4.2.11
Configure the Switch

Do the following to configure a switch using the SANbox Manager application. Refer to the *SANbox2-8c/16 Switch Management User's Guide* for more information about configuring a switch. You can also configure the switch using the Command Line Interface. Refer to Appendix B Command Line Interface for more information.

1. Connect to the switch using an Ethernet connection and run SANbox Manager.
2. Open the Fabric menu and select **Add Fabric** to open the Add a New Fabric window.

3. Enter a fabric name and the IP address of the switch through which to manage the fabric. The default IP address is 10.0.0.1. If this is a new switch, leave the login name and password fields empty, and choose the **Add Fabric** button. By default, user authentication is disabled, and therefore, the Admin account name and password are used. Refer to the "Set Setup Command" on page B-54 for information about setting fabric security.
4. Open the Switch menu and select **Switch Properties**. In the Switch Properties window, enter a chassis name. Accept the default domain ID, and choose the **OK** button.
5. Open the Switch menu and select **Network Properties**. In the Network Properties window, enter values for the IP address, subnet mask, and gateway address. Accept the default boot method. If you know the SNMP configuration settings, enter those as well. Choose the **OK** button.
6. Set the date and time. Double click on the switch in the topology display. In the faceplate display, open the Switch menu and select **Set Date/Time**. Enter the date and time in the Switch Date and Time window and choose the **OK** button. Reset the switch when prompted to implement the new and date and time.

Repeat this process for each switch in the fabric, then connect the switches.

4.2.12 Configure the Ports

Configuring a port involves defining the port mode. For devices and other switches, a switch automatically sets the port mode as each port discovers the type of device to which it is connected. The default port mode is GL_Port.

A GL_Port will self configure as an FL_Port when connected to a loop of public devices or an F_Port when connected to a single public device. A G_Port will self configure as an F_Port when connected to a single public device. Both GL_Ports and G_Ports self configure as E_Ports when connected to another switch. Refer to the *SANbox2-8c/16 Switch Management User's Guide* for more information about configuring ports. You can also configure ports using the CLI. Refer to Appendix B Command Line Interface for more information.

4.2.13 Cable Devices to the Switch

Connect cables to the SFP transceivers and their corresponding devices, and then energize the devices. Device host bus adapters can have SFP (or SFF) transceivers or GigaBit Interface Converters (GBIC). LC-type duplex fiber optic cable connectors are designed for SFP transceivers, while SC-type connectors are designed for GBICs. Duplex cable connectors are keyed to ensure proper orientation. Choose the fiber optic cable with the connector combination that matches the device host bus adapter.

4.3 Install Firmware

The switch comes with current firmware installed. You can upgrade the firmware from the management workstation as new firmware becomes available. Firmware installation involves loading the firmware image file onto the switch, unpacking the image file, and then resetting the switch to activate the new firmware. Firmware versions that follow version 2.0 can be loaded and activated on an operating switch without disrupting traffic.

You can use the SANbox Manager application or the CLI to install new firmware:

- The SANbox Manager application loads and unpacks the firmware image file in one operation. Refer to ”Using SANbox Manager to Install Firmware” on page 4-17.
- When using the CLI on a workstation that has an FTP server, you can open a Telnet session and load and unpack the firmware image file using the CLI Image command. Refer to ”Using the CLI to Install Firmware” on page 4-18.
- When using the CLI on a workstation without an FTP server, you must open an FTP session through the switch to load the image file, then open a Telnet session to unpack it with the CLI Image command. Refer to ”Using FTP and the CLI to Install Firmware” on page 4-19.

4.3.1 Using SANbox Manager to Install Firmware

To install firmware using SANbox Manager, do the following:

1. From the Faceplate display, open the Switch menu and select **Load Firmware**.
2. In the Firmware Upload window, browse and select the firmware file you want to load.
3. In the Firmware Upload window, choose the **Start** button to begin the loading process. When the firmware is finished loading, the Bytes Transferred field displays the number of bytes that have been transferred.
4. Choose the **Close** button to close the Firmware Upload window.
5. If a non-disruptive activation is not possible, SANbox Manager prompts you to reset the switch. Choose the **OK** button to reset the switch and activate the new firmware.

4.3.2
Using the CLI to Install Firmware

To install firmware using the CLI when an FTP server is present on the management workstation, do the following:

1. Connect to the switch through the Ethernet or the serial port and open a Telnet session.
2. Enter the following account name and password:

   ```
   SANbox2 Login:admin
   Password: password
   ```

3. To start an admin session, enter the following:

   ```
   SANbox2 $> admin start
   ```

4. Retrieve the firmware file. The device on which the firmware file is stored must be running an FTP server. Enter the following command to retrieve the firmware file from the specified IP address:

   ```
   SANbox2 (admin) #> image fetch username 10.0.0.254
   firmwarefilenametoload firmwarefilenameonswitch
   Connected to 10.0.0.254.
   ```

   Note: If prompted for your password, enter your password (for that IP Address) and press the Enter key.

   ```
   331 Password required for username.
   Password:
   230 User username logged in.
   bin
   200 Type set to I.
   verbose
   Verbose mode off.
   ```

5. Enter the following command to display the list of firmware files:

   ```
   SANbox2 (admin) #> image list
   ```

6. Enter the following command to install the new firmware:

   ```
   SANbox2 (admin) #>image unpack filename
   ```

7. If the new firmware is version 2.0 or later, the new firmware can be acivated without disrupting traffic. Enter the Hotreset command to perform a non-disruptive activation.

   ```
   SANbox2 (admin) $>hotreset
   ```

4.3.3
Using FTP and the CLI to Install Firmware

To install firmware using the CLI when the management workstation does not have an FTP server, do the following:

1. Connect to the switch through the Ethernet or the serial port.
2. Move to the folder or directory that contains the new firmware image file.
3. Establish communications with the switch using the File Transfer Protocol (FTP). Enter one of the following on the command line:

   ```
   >ftp xxx.xxx.xxx.xxx
   ```

   or

   ```
   >ftp switchname
   ```

   where *xxx.xxx.xxx.xxx* is the switch IP address, and *switchname* is the switch name associated with the IP address.
4. Enter the following account name and password:

   ```
   user:images
   password: images
   ```
5. Activate binary mode and copy the firmware image file on the switch:

   ```
   ftp>bin
   ftp>put filename
   ```
6. Close the FTP session.

   ```
   ftp>quit
   ```
7. Establish communications with the switch using the CLI. Enter one of the following on the command line:

   ```
   telnet xxx.xxx.xxx.xxx
   ```

   or

   ```
   telnet switchname
   ```

   where *xxx.xxx.xxx.xxx* is the switch IP address, and *switchname* is the switch name associated with the IP address.
8. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are (admin, password).
9. Open an Admin session to acquire the necessary authority.

   ```
   SANbox2 $>admin start
   ```

10. Display the list of firmware image files on the switch to confirm that the file was loaded. Refer to the ”Image Command” on page B-21 for more information.

```
SANbox2 (admin) $>image list
```

11. Unpack the firmware image file to install the new firmware in flash memory.

```
SANbox2 (admin) $>image unpack filename
```

12. If the new firmware is later than version 2.0, the new firmware can be activated without disrupting traffic. Enter the Hotreset command to perform a non-disruptive activation.

```
SANbox2(admin) $>hotreset
```

4.4 Powering Down a Switch

Simply unplugging the switch from the power source does not allow the switch to complete executing tasks and could lead to flash memory corruption. For this reason, open a Telnet session and use the Shutdown command to initiate an orderly shut down, then power down the switch. Refer to the ”Shutdown Command” on page B-82.

Section 5

Diagnostics/Troubleshooting

Diagnostic information about the switch is available through the chassis LEDs, the power supply LEDs, and the Logged-In LED. Diagnostic information is also available through the SANbox Manager and CLI event logs and error displays. This section describes two types of diagnostics: Power On Self Test (POST) and chassis. POST diagnostics describe the Heartbeat LED and the port Logged-In LED indications. Chassis diagnostics cover power supply and fan diagnostics as well as over temperature conditions. This section also describes how to use maintenance mode to recover a disabled switch.

5.1 POST Diagnostics

The switch performs a series of Power On Self Tests (POST) as part of its power-up procedure. The POST diagnostic program performs the following tests:

- Checksum tests on the boot firmware in PROM and the switch firmware in flash memory
- Internal data loopback test on all ports
- Access and integrity test on the ASIC

During the POST, the switch logs any errors encountered. Some POST errors are fatal, others are non-fatal. The switch uses the Heartbeat LED and the Logged-In LED to indicate switch and port status. A fatal error disables the switch so that it will not operate. A non-fatal error allows the switch to operate, but disables the ports that have errors. Whether the problem is fatal or non-fatal, contact your authorized maintenance provider.

If there are no errors, the Heartbeat LED blinks at a steady rate of once per second. If a fatal error occurs, the Heartbeat LED will show an error blink pattern. If there are non-fatal errors, the switch disables the failed ports and flashes the associated Logged-In LEDs. Refer to ”Heartbeat LED Blink Patterns” on page 5-1 for more information about Heartbeat LED blink patterns.

5.1.1 Heartbeat LED Blink Patterns

5.1.1.1 Normal (all pass)

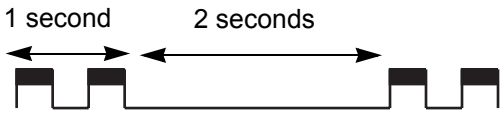
If all POST diagnostics pass, the switch will go to normal operation and the Heartbeat LED will blink at a steady rate of one (1) blink per second.

5.1.1.2
Maintenance Mode Pattern

Steady illumination indicates that the switch is in maintenance mode, which returns the switch IP address to 10.0.0.1. From maintenance mode, you may reload firmware, reset the password to the factory default, and remove a corrupt configuration.

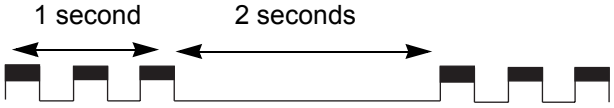
5.1.1.3
Internal Firmware Failure Blink Pattern

An internal firmware failure blink pattern is 2 blinks per second followed by a two second pause. The 2-blink error pattern indicates that the firmware has failed, and that the switch must be reset. Power cycle the switch to reset it.



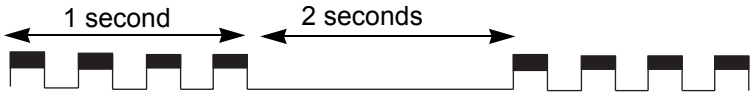
5.1.1.4
Fatal Error Blink Pattern

A fatal error blink pattern is 3 blinks per second followed by a two second pause. The 3-blink error pattern indicates that a fatal error has left the switch inoperable. If a fatal error occurs, contact your authorized maintenance provider. Power cycle the switch to reset the switch.



5.1.1.5
Configuration File System Error Blink Pattern

A configuration file system error blink pattern is 4 blinks per second followed by a two second pause. The 4-blink error pattern indicates that a configuration file system error has occurred, and that the configuration file must be recreated. Refer to ”Recovering a Switch” on page 5-12 for more information.



To recreate the configuration file, do the following:

1. Open a Telnet session and use the Shutdown command to close activity on the switch, then power down the switch. Refer to the ”Shutdown Command” on page B-82.

2. Place the switch in maintenance mode. Press and hold the Maintenance button, then power up the switch. Refer to ”Recovering a Switch” on page 5-12 for more information about placing the switch in maintenance mode.
3. Establish a Telnet session with the switch using the default IP address 10.0.0.1.

```
telnet 10.0.0.1
```

4. Enter the account name (prom) and password (prom), and press the Enter key.

```
Sanbox2 login: prom
Password:xxxx
[username@host:Itasca]% telnet 10.0.0.1
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
```

5. The following menu is displayed. Enter "6" (Remake Filesystem) and press the Enter key to recreate the configuration file.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset Password File
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
8)  Show Firmware Versions
9)  Set Active Image
Option: 6
```

6. When the recreate process is complete, select option 7 to reset the switch and exit maintenance mode.
7. If a previously saved configuration file is available for the switch, do the following to restore the configuration file.
   a. Establish communications with the switch using the File Transfer Protocol (FTP). Enter one of the following on the command line:

```
>ftp xxx.xxx.xxx.xxx
```

   or

```
>ftp switchname
```

   where *xxx.xxx.xxx.xxx* is the switch IP address and *switchname* is the switch name associated with the IP address.

b. Enter the following account name and password:

```
user:images
password:images
```

c. Activate binary mode and copy the configuration file from the workstation to the switch. The configuration file must be named "configdata".

```
ftp>bin
ftp>put configdata
```

d. Close the FTP session.

```
ftp>quit
```

e. Establish communications with the switch using Telnet. Enter one of the following on the command line:

```
telnet xxx.xxx.xxx.xxx
```

or

```
telnet switchname
```

where *xxx.xxx.xxx.xxx* is the switch IP address and *switchname* is the switch name associated with the IP address.

f. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are (admin, password).

g. Open an admin session to acquire the necessary authority.

```
SANbox2 $>admin start
```

h. Restore the configuration file.

```
SANbox2 (admin) $>config restore
```

i. Reset the switch and close the Telnet session.

```
SANbox2 (admin) $>reset
```

5.1.2
Logged-In LED Indications

Port diagnostics are indicated by the Logged-In LED for each port as shown in Figure 5-1.

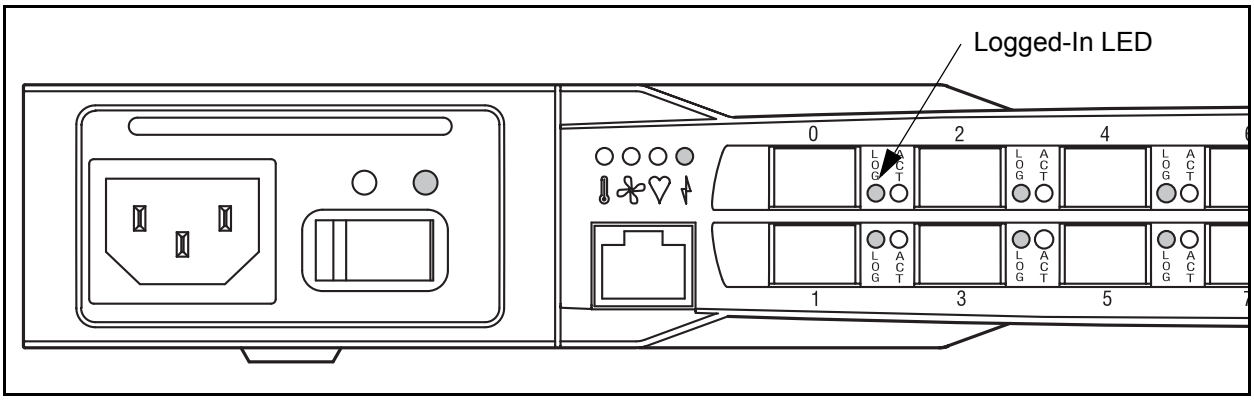


Figure 5-1. Logged-In LED

The Logged-In LED has three indications:

- Logged in - Continuous illumination.
- Logging in - Flashes at roughly once per second as shown in Figure 5-2.
- Error - Flashes at roughly twice per second as shown in Figure 5-2.

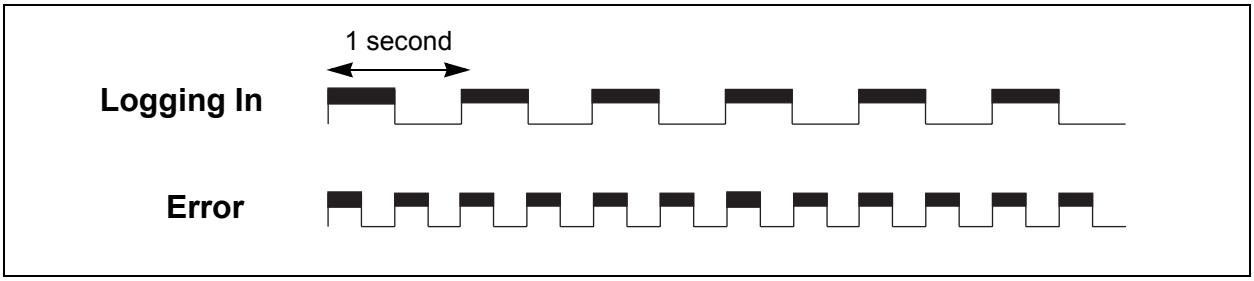


Figure 5-2. Logged-In LED Indications

If a Logged-In LED shows an error indication, review the event browser for alarm messages regarding the affected port. You can also inspect the event log using the Show Alarm command. Pertinent alarm messages will point to one or more of the following conditions:

- E_Port isolation
- Excessive port errors

5.1.2.1
E_Port Isolation

A Logged-In LED error indication is often the result of E_Port isolation. An isolated E_Port is indicated by a red link in the SANbox Manager topology display. E_Port isolation can be caused by a security failure, conflicting domain IDs, conflicting timeout values, or conflicting zone membership between active zone sets. Refer to the *SANbox2-8c/16 Switch Management User's Guide* for information about how to change domain IDs, timeout values, and edit zoning.

Review the event browser and do the following to diagnose and correct an isolated E_Port:

1. Does the event browser show an alarm for an invalid attach for the affected port?
   - Yes - Review the ISL group in the active security set to ensure that the membership includes the necessary ports and that the secrets on all switches are correct.
   - No - Continue.
2. Display the fabric domain IDs using the Show Domains command or the Switch data tab in the SANbox Manager topology display. Are all domain IDs in the fabric unique?
   - Yes - Continue.
   - No - Correct the domain IDs on the offending switches using the Set Config Switch command or the SANbox Manager Switch Properties window. Reset the port. If the condition remains, continue.
3. Compare the RA_TOV and ED_TOV timeout values for all switches in the fabric using the Show Config Switch command or the Switch data tab of the SANbox Manager topology display. Is each timeout value the same on every switch?
   - Yes - Continue.
   - No - Correct the timeout values on the offending switches using the Set Config Switch command or the SANbox Manager Switch Properties dialog. Reset the port. If the condition remains, continue.
4. Display the active zone set on each switch using the Zoning Active command or the Active Zoneset tab of the SANbox Manager topology display. Compare the zone membership between the two active zone sets. Are they the same?
   - Yes - Contact your authorized maintenance provider.
   - No - Deactivate one of the active zone sets or edit the conflicting zones so that their membership is the same. Reset the port. If the condition remains, contact your authorized maintenance provider.

Note: This can be caused by merging two fabrics whose active zone sets have two zones with the same name, but different membership.

5.1.2.2

Excessive Port Errors

The switch monitors a set of port errors and generates alarms based on user-defined sample intervals and thresholds. Refer to the *SANbox2-8c/16 Switch Management User's Guide* for information about managing alarms. These port errors include the following:

- CRC errors
- Decode errors
- ISL connection count
- Login errors
- Logout errors
- Loss-of-signal errors

If the count for any of these errors exceeds the rising threshold for three consecutive sample intervals, the switch generates an alarm and disables the affected port, changing its operational state to "down". Port errors can be caused by the following:

- Thresholds are too low or the sample interval is too small
- Faulty Fibre Channel port cable
- Faulty SFP
- Faulty port
- Fault device or HBA

Review the event browser to determine if excessive port errors are responsible for disabling the port. Look for a message that mentions one of the monitored error types indicating that the port has been disabled, then do the following:

1. Examine the alarm configuration for the associated error using the Show Config Threshold command or the SANbox Manager application. Refer to the ”Show Config Command” on page B-72. Refer to Table B-7 for a list of the alarm configuration defaults. Are the thresholds and sample interval correct?
   - Yes - Continue
   - No - Correct the alarm configuration. If the condition remains, continue.
2. Reset the port, then perform an external port loopback test to validate the port and the SFP. Refer to the ”Test Command” on page B-83 or the *SANbox2-8c/16 Switch Management User’s Guide* for information about testing ports. Does the port pass the test?
   - Yes - Continue
   - No - Replace the SFP and repeat the test. If the port does not pass the test, contact your authorized maintenance provider. Otherwise continue.
3. Replace the Fibre Channel port cable. Is the problem corrected?
   - Yes - Complete.
   - No - Continue.
4. Inspect the device to which the affected port is connected and confirm that the device and its HBA are working properly. Make repairs and corrections as needed. If the condition remains, contact your authorized maintenance provider.

5.2 Chassis Diagnostics

Chassis diagnostics are indicated by the chassis and power supply LEDs as shown in Figure 5-3.

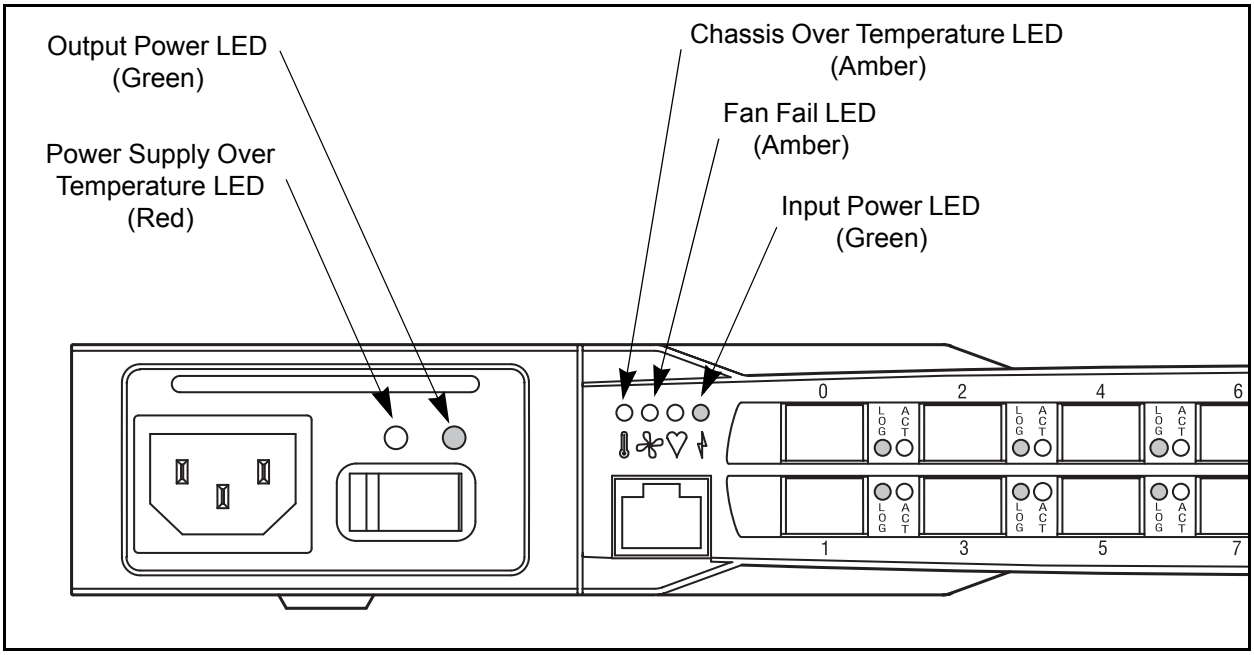


Figure 5-3. Chassis and Power Supply LEDs

The following conditions are described:

- Chassis Over Temperature LED is illuminated
- Input Power LED is extinguished
- Fan Fail LED is illuminated
- Output Power LED is extinguished
- Power supply Over Temperature LED is illuminated

Note: The chassis and power supply Over Temperature LEDs are different. The chassis LED indicates an over temperature condition in the switch logic circuitry; the power supply LED indicates an over temperature condition in the power supply.

5.2.1
Chassis Over Temperature LED is Illuminated

The chassis Over Temperature LED illuminates to indicate that the switch logic circuitry is overheating. If the chassis Over Temperature LED illuminates, do the following:

1. Inspect the chassis fans. Are the intake openings clear? Are all fans operating and producing air flow?
   - Yes - Continue.
   - No - Remove any debris from fan intakes and exhausts if necessary. Replace any fan that is not operating. Refer to Section 6 Removal/Replacement. If the condition remains, continue.
2. Consider the ambient air temperature near the switch. Make necessary corrections. If the condition remains, shut down the switch immediately and contact your authorized maintenance provider.

5.2.2
Input Power LED Is Extinguished

The Input Power LED illuminates to indicate that the switch logic circuitry is receiving proper voltages. If the Input Power LED is extinguished, inspect the Output Power LED. Is the Output Power LED illuminated?

- Yes - Contact your authorized maintenance provider.
- No - Refer to ”Output Power LED Is Extinguished” on page 5-11.

5.2.3
Fan Fail LED is Illuminated

The Fan Fail LED illuminates to indicate a malfunction with one or more of the chassis fans. If the Fan Fail LED illuminates, do the following:

1. Inspect the chassis fan connections. Remove and reinstall the chassis fan. Refer to Section 6 Removal/Replacement. If the condition remains, continue.
2. Are all fans operating and producing equal air flow?
   - Yes - Contact your authorized maintenance provider.
   - No - Replace the weaker chassis fan. Refer to Section 6 Removal/Replacement. If the condition remains, contact your authorized maintenance provider.

Note: Removing a fan will not illuminate the Fan Fail LED.

5.2.4
Output Power LED Is Extinguished

The Output Power LED illuminates to indicate that the power supply is producing the proper voltages. If the Output Power LED is extinguished, do the following:

1. Inspect the power supply Over Temperature LED. Is the power supply Over Temperature LED illuminated?
   - Yes - Refer to ”Power Supply Over Temperature LED is Illuminated” on page 5-11.
   - No - Continue.
2. Inspect the power cables and connectors. Are the cables unplugged? Are the cables or connectors damaged?
   - Yes - Make necessary corrections or repairs. If the condition remains, continue.
   - No - Continue.
3. Inspect the power source. Is the power source delivering the proper voltage?
   - Yes - Continue
   - No - Make necessary repairs. If the condition remains, continue.
4. Replace the power supply. Refer to Section 6 Removal/Replacement. If the condition remains, contact your authorized maintenance provider.

5.2.5
Power Supply Over Temperature LED is Illuminated

The power supply Over Temperature LED illuminates to indicate that the power supply is overheating. If the power supply Over Temperature LED illuminates, do the following:

1. Inspect the chassis fans. Are the intake openings clear? Are both fans operating and producing air flow?
   - Yes - Continue.
   - No - Remove any debris from fan intakes if necessary. Replace any fan that is not operating. Refer to Section 6 Removal/Replacement. If the condition remains, continue.
2. Consider the ambient air temperature near the switch and clearance around the switch. Make necessary corrections. If the condition remains, continue.
3. Replace the power supply. Refer to Section 6 Removal/Replacement. If the condition remains, contact your authorized maintenance provider.

5.3
Recovering a Switch

A switch can become inoperable or unmanageable for the following reasons:

- Firmware becomes corrupt
- IP address is lost
- Switch configuration becomes corrupt
- Forgotten password

In these specific cases, you can recover the switch using maintenance mode. Maintenance mode temporarily returns the switch IP address to 10.0.0.1 and provides opportunities to do the following:

- Unpack a firmware image file
- Restore the network configuration parameters to the default values
- Remove all user accounts and restore the Admin account name password to the default.
- Copy the log file
- Restore factory defaults for all but user accounts and zoning
- Restore all switch configuration parameters to the factory default values
- Reset the switch
- Display firmware versions stored on the switch
- Select the firmware image to activate

To recover a switch, do the following:

1. Place the switch in maintenance mode. Do the following:
    a. Power down the switch.
    b. Press and hold the Maintenance button with a pointed tool, then power up the switch. All chassis LEDs will illuminate, then extinguish leaving only the Input Power LED illuminated. Release the button.
2. Allow one minute for the switch to complete its tests. When the switch is in maintenance mode, the Input LED will be illuminated and the Heartbeat LED will illuminate continuously. All other chassis LEDs will be extinguished.
3. Establish a Telnet session with the switch using the maintenance mode IP address 10.0.0.1.

4. Enter the maintenance mode account name and password (prom, prom), and press the Enter key.

```
Sanbox login: prom
Password:xxxx
[username@anteater:Itasca]% telnet 10.0.0.1
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
```

5. The maintenance menu displays several recovery options. To select a switch recovery option, press the corresponding number (displayed in option: field) on the keyboard and press the Enter key.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset Password File
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
8)  Show Firmware Versions
9)  Set Active Image
Option:
```

These options and their use are described in the following subsections.

5.3.1 Maintenance – Exit

This option closes the current login session. To log in again, enter the maintenance mode account name and password (prom, prom). To return to normal operation, power cycle the switch.

5.3.2
Maintenance – Image Unpack

This option unpacks and installs new firmware when the current firmware has become corrupt. Before using this option, you must load the new firmware image file onto the switch. The steps to install new firmware using this option are as follows:

1. Place the switch in maintenance mode. Refer to the procedure for maintenance mode in ”Recovering a Switch” on page 5-12.
2. Use FTP to load a new firmware image file onto the switch. Refer to ”Using FTP and the CLI to Install Firmware” on page 4-19. Do not unpack the firmware image file with the Image command.
3. Select option 1 from the maintenance menu. When prompted for a file name prompt, enter the firmware image file name.

```
Image filename: filename
Unpacking 'filename', please wait...
Unpackage successful.
```

4. Select option 7 to reset the switch and exit maintenance mode.

5.3.3
Maintenance – Reset Network Config

This option resets the network properties to the factory default values and saves them on the switch. Refer to Table B-10 for the default network configuration values.

5.3.4
Maintenance – Reset Password File

This option restores the password for the Admin account name to the default (password) and removes all other user accounts from the switch.

5.3.5
Maintenance – Copy Log Files

This option copies all log file buffers to a file on the switch named *logfile*. You can use FTP to download this file to the management workstation.

5.3.6
Maintenance – Remove Switch Config

This option deletes all configurations from the switch except for the default configuration. This restores switch configuration parameters to the factory defaults except for user accounts and zoning. Refer to Table B-5 though Table B-10 for the factory default values.

5.3.7
Maintenance – Remake Filesystem

In the event of sudden loss of power, it is possible that the switch configuration may become corrupt. The file system on which the configuration is stored must be re-created. This option resets the switch to the factory default values including user accounts and zoning. Refer to Table B-5 though Table B-10 for the factory default values.

CAUTION! If you choose the **Remake Filesystem** option, you will lose all changes made to the fabric configuration that involve that switch, such as password and zoning changes. You must then reconfigure the portions of the fabric that involve the switch.

5.3.8
Maintenance – Reset Switch

This option closes the Telnet session, exits maintenance mode and reboots the switch using the current switch configuration. All unpacked firmware image files that reside on the switch are deleted.

5.3.9
Maintenance – Show Firmware Versions

This option displays the image numbers and firmware versions that are stored on the switch.

5.3.10
Maintenance – Set Active Image

This option specifies the firmware version to be used when the switch returns to normal operation. A message reminds you of the pending firmware version and gives you an opportunity to change it by selecting the other image number.

Notes

Section 6
Removal/Replacement

This section describes the removal and replacement procedures for the following field replaceable units (FRU):

- SFP transceivers
- Power supplies
- Fans

The switch is equipped with a battery that powers the non-volatile memory. This memory stores the switch configuration. The battery is not a field replaceable unit.

WARNING!! Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of the used battery according to the manufacturer's instructions.

WARNUNG!!

Bei unsachgemäß ausgetauschter Batterie besteht Explosionsgefahr. Die Batterie nur mit der gleichen Batterie oder mit einem äquivalenten, vom Hersteller empfohlenen Batterietyp ersetzen. Die gebrauchte Batterie gemäß den Herstelleranweisungen entsorgen.

AVERTISSEMENT!!

Danger d'explosion si le remplacement de la pile est incorrect. Ne remplacer que par une pile de type identique ou équivalent recommandé par le fabricant. Jeter la pile usagée en observant les instructions du fabricant.

6.1 SFP Transceivers

The SFP transceivers can be removed and replaced while the switch is operating without damaging the switch or the transceiver. However, transmission on the affected port will be interrupted until the transceiver installed.

To remove a transceiver, gently press the transceiver into the port to release the tension, then pull on the release tab or lever and remove the transceiver. Different transceiver manufacturers have different release mechanisms. Consult the documentation for your transceiver. To install, insert the transceiver into the port and gently press until it snaps in place as shown in Figure 6-1.

Note: The SFP transceiver will fit only one way. If the SFP does not install under gentle pressure, flip it over and try again.

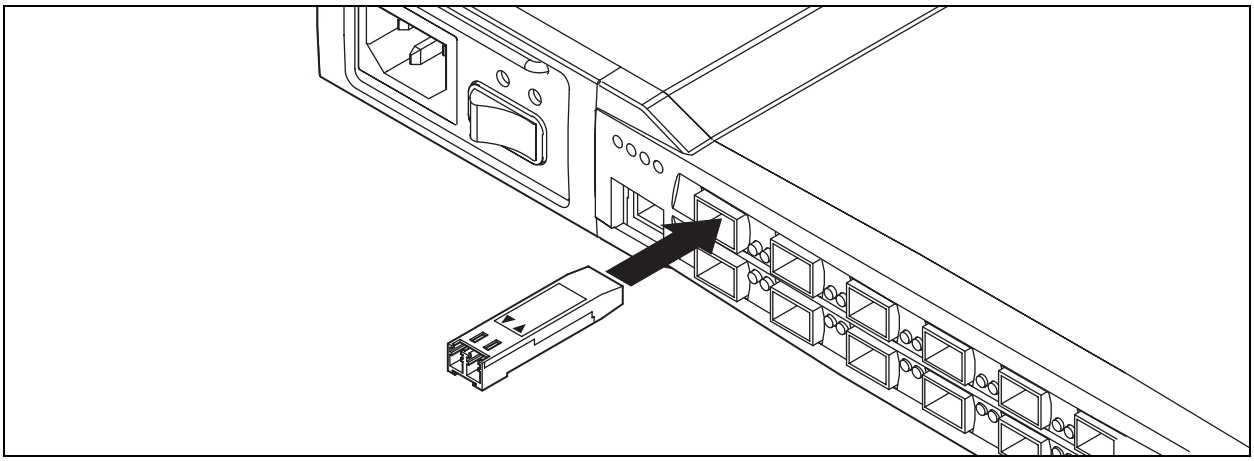


Figure 6-1. SFP Transceiver Installation

6.2
Power Supplies

The power supplies are hot pluggable. This means you can remove or install one of the power supplies while the switch is operating without disrupting service. The power supplies are also interchangeable; that is, the left and right power supplies are the same unit.

To remove the power supply, grasp the power supply latch handle and pull firmly to release the latches and disengage the modular connector. Slide the power supply out of its bay as shown in Figure 6-2.

To install a power supply, slide the power supply into the bay with the latch handle on top. Press the power supply firmly into place until it is fully seated, then push the latch handle in against the power supply to engage the latches.

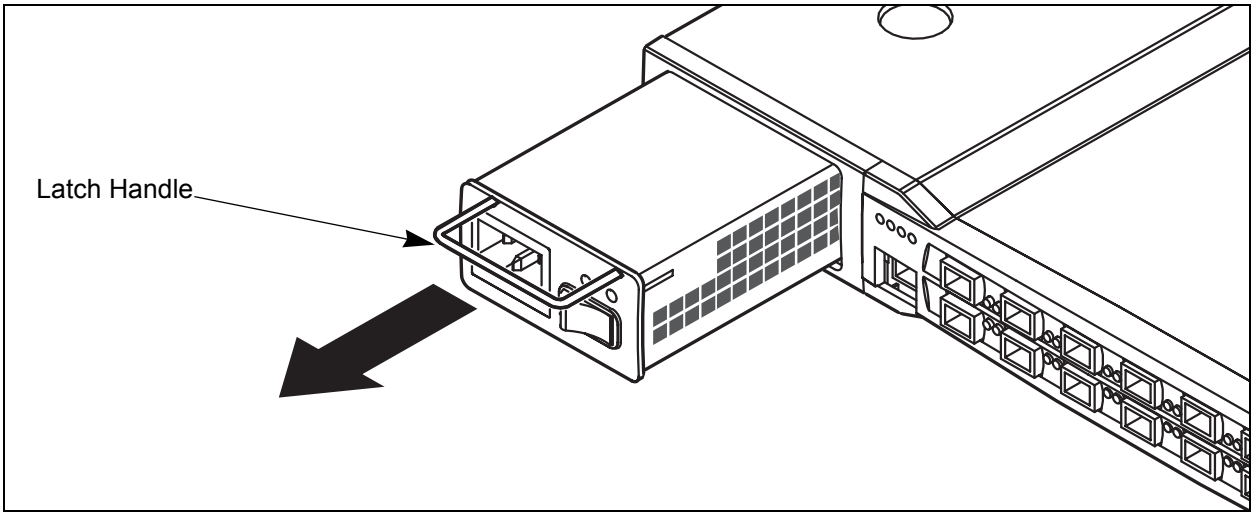


Figure 6-2. Power Supply Removal

6.3 Fans

The fans are hot pluggable. This means you can remove or install one of the fans while the switch is operating without disrupting service. The fan is completely enclosed, so there is no risk of injury from the fan blades. The fans are also interchangeable; that is, the left and right fans are the same unit.

To remove a fan, loosen the two retaining screws, then grasp the fan housing and pull firmly to disengage the modular connector. Slide the fan out of its bay as shown in Figure 6-2.

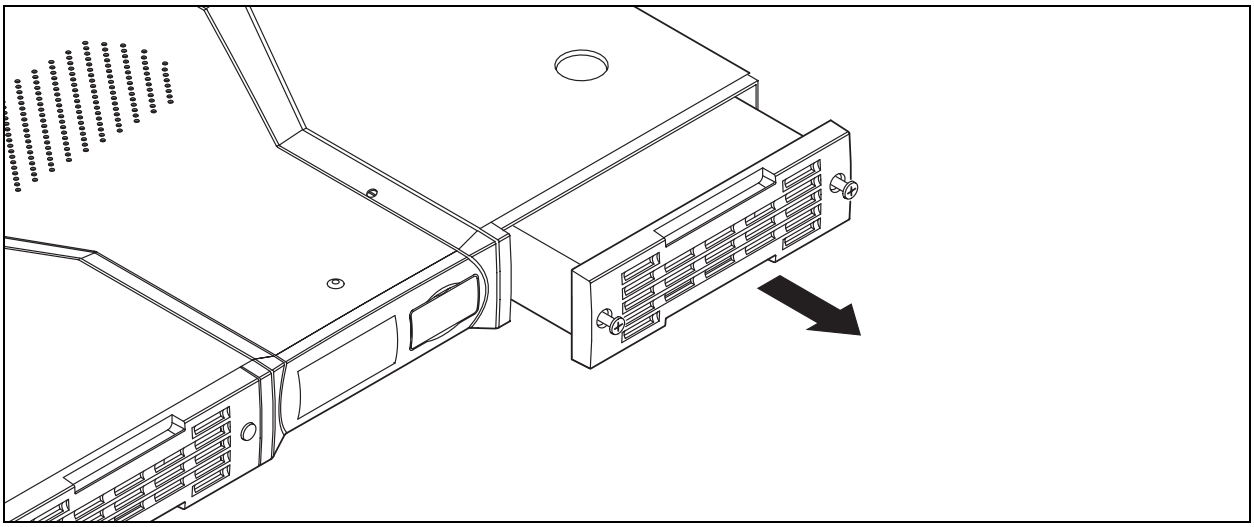


Figure 6-3. Fan Removal

When replacing a fan, consider the following:

- The left and right fans are interchangeable. However, you must orient the fan so that the modular connector aligns with the mating connector in the switch as shown in Figure 6-4.
- Replacement fans must be compatible with the switch air flow direction. Air flow direction for switch model SB2A-16A is front-to-back; air flow direction for switch model SB2A-16B is back-to-front.
- A label on the fan indicates the switch model number and fan air flow direction as shown in Figure 6-4.

CAUTION! Both fans must have the same air flow direction to prevent the switch from overheating.

To install a fan, do the following:

1. Confirm that the new fan is compatible with the switch air flow direction.

2. Align the modular connector toward the inside of the switch as shown in Figure 6-4.
3. Slide the fan into the bay until it is firmly seated and confirm that the air flow is correct. Fasten the screws.

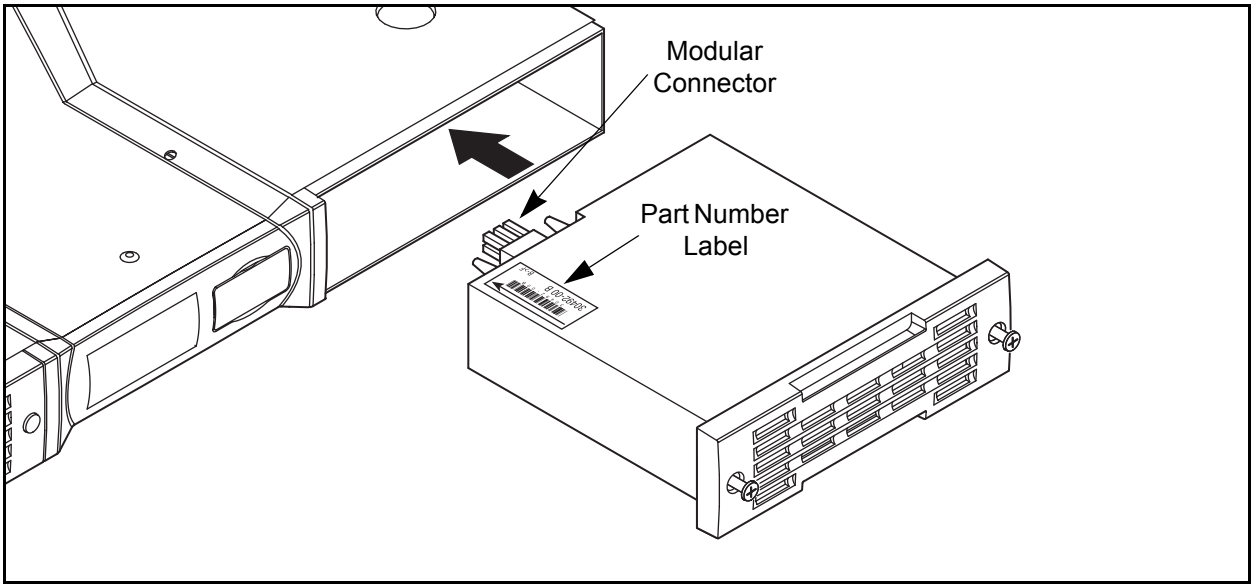


Figure 6-4. Fan Installation for Switch Model SB2A-16B

Notes

Appendix A
Specifications

This appendix contains the specifications for the SANbox2-16 Fibre Channel switch. Refer to Section 2 General Description for the location of all connections, switches, controls, and components.

A.1 Fabric Specifications

Fibre Channel Protocols	FC-PH Rev. 4.3 FC-PH-2 FC-PH-3 FC-AL Rev 4.5 FC-AL-2 Rev 7.0 FC-FLA FC-GS-3 FC-FG FC-Tape FC-VI FC-SW-2 Fibre Channel Element MIB RFC 2837 Fibre Alliance MIB Version 4.0
Fibre Channel Classes of Service ..	Classes 2 and 3
Modes of Operation	Fibre Channel Classes 2 and 3, connectionless
Port Types.....	F_Port FL_Port E_Port G_Port GL_Port
Port Characteristics	All ports are auto-discovering and self-configuring.
Number of Fibre Channel Ports	16 ports per chassis
Scalability.....	Maximum 239 switches depending on configuration
Maximum User Ports	> 475,000 ports depending on configuration

Buffer Credits	12 buffer credits per port
Media Type	Small Form Pluggable (SFP) optical transceivers. Hot swappable. 3.3 Volts.
Fabric Port Speed	1.0625 or 2.125 Gigabits/second
Maximum Frame Size	2148 bytes (2112 byte payload)
System Processor	266 MHz Pentium® processor
Fabric Latency (best case)	<0.4 µsec.
Fabric Point-to-Point Bandwidth	212 or 424 MB/s full duplex
Fabric Aggregate Bandwidth	64 Gb/s for a single switch

A.2 Maintainability

Maintenance Strategy	Field Replaceable Units ■ SFP transceivers ■ Power supplies ■ Fans
Diagnostics	Power On Self Test (POST) tests all functional components except SFP transceivers. Port tests include online, internal, and external tests.
User Interface	LED indicators

A.3 Fabric Management

Management Methods	SANbox Manager Graphical User Interface Application Programming Interface Command Line Interface GS-3 Management Server SNMP FTP
Maintenance Connection	RS-232 connector; null modem F/F DB9 cable
Ethernet Connection	RJ-45 connector; 10/100 BASE-T cable
Switch Agent	Allows a network management station to obtain configuration values, traffic information, and failure data pertaining to the Fibre Channels using SNMP through the Ethernet interface.

A.4 Dimensions

Width	17.0” (431 mm), 19 inch rack mount
Height	1.75” (44 mm) (1U)
Depth	18.0” (457 mm)
Weight	18 lbs (8.16 Kg)

A.5 Electrical

Operating voltage	90 to 137 Vac; 47 to 63 Hz 180 to 265 Vac; 47 to 63 Hz
Power source loading	1.9 Amps maximum at 90 to 137 Vac 0.95 Amps maximum at 180 to 265 Vac
Heat Output (maximum)	170 watts
Circuit Protection	Internally fused

A.6
Environmental

Temperature	
■ Operating	10 to 40°C (50 to 104°F)
■ Non-operating	-40 to 65°C (-40 to 149°F)
Humidity	
■ Operating	25% to 80%, non-condensing
■ Non-operating	25% to 90%, non-condensing
Altitude	
■ Operating	0 to 3048m (0 to 10,000 feet)
■ Non-operating	0 to 15,240m (0 to 50,000 feet)
Vibration	Magnitude during/after along any axis
■ Operating	2.54 mm (.1); 5 - 14 Hz 0.1G; 14-300 Hz
■ Non-operating	5 - 500 Hz, random 2.09 G rms, 10 minutes
Shock	Magnitude during/after along any axis
■ Operating	1 g for 15 msec
■ Non-operating	8 g for 15 msec
Air flow	Two fans; front-to-back or back-to-front by model

A.7 Regulatory Certifications

Safety Standards	UL1950, CSA 22.2 No. 950, EN60950
Emissions Standards	FCC Part 15B Class A VCCI Class A ITE BSMI Class A CISPR 22, Class A EN 55022, Class A
Voltage Fluctuations	EN 61000-3-3
Harmonics.....	EN 61000-3-2
Immunity	EN 55024:1998
Marking	FCC Part 15,UL (United States), cUL (Canada), TUV, VCCI, BSMI, CE
SANmark®	SCD 3001, 3002, 3010, 3020

A.8
Shortwave Laser SFP 1G/2G (multi-mode)

Connector	Duplex LC
Color coding	Beige or black exposed connector surfaces
Cable	Fibre Channel 100-M6-SN-I (50 µm multimode) Fibre Channel 200-M5-SN-I or 200-M6-SN-I (62.5 µm multimode)
Wavelength	830 - 860 nm
Transmit Power	-10 dBm minimum
Receiver Sensitivity	-16 dBm average
Distance	500 meters maximum, 50 micron fiber 300 meters maximum, 62.5 micron fiber
Safety	DHHS 21 CFR(J), IEC 825-1 CENELEC EN 60825-1, VDE
Standard	Small Form-Factor Pluggable Multisource Agreement

A.9 Longwave Laser SFP 1G/2G (single-mode)

Connector	Duplex LC
Color coding	Blue exposed connector surfaces
Cable	Fibre Channel 100SM-LC-L (9 µm single mode)
Wavelength	1270 - 1350 nm
Transmit Power	-10 dBm minimum
Receiver Sensitivity	-20 dBm average
Distance	2 meters to 10 kilometers
Safety	DHHS 21 CFR(J), IEC 825-1 CENELEC EN 60825-1, VDE
Standard	Small Form-Factor Pluggable Multisource Agreement

Notes

Appendix B
Command Line Interface

Each switch contains a Telnet server. This server allows a Telnet client to establish a Telnet session with the switch to retrieve information or to configure parameters using the Command Line Interface (CLI). The CLI enables you to perform a variety of fabric and switch management tasks through an Ethernet or a serial port connection.

B.1 Logging On to a Switch

To log on to a switch using Telnet, open a command line window on the management workstation and enter the Telnet command followed by the switch IP address:

```
/> telnet 123.45.67.89
```

A Telnet window opens prompting you for a login. Enter an account name and password. Switches come from the factory with the following user account already defined:

Account name: admin
Password: password
Authority: Admin

This user account provides full access to the switch and its configuration. After planning your fabric management needs and creating your own user accounts, consider changing the password for this account. Refer to ”Commands” on page B-3 for more information about authority levels. Refer to the ”User Command” on page B-87 for information about creating user accounts.

Note: A switch supports a combined maximum of 19 logins reserved as follows:

- 4 sessions for internal applications such as management server and SNMP
- 15 sessions for SANbox Manager inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins and Telnet logins. Of these 15, there can be a combined maximum of 10 SANbox Manager and API logins. Additional logins will be refused.

B.2 Command Syntax

The command syntax is as follows:

command
keyword
keyword *[value]*
keyword [value1] [value2]

The **Command** is followed by one or more keywords. Consider the following rules and conventions:

- Commands and keywords are case insensitive.
- Required keyword values appear in standard font: [value]. Optional values are shown in italics: *[value].*
- Underlined portions of the keyword in the command format indicate the abbreviated form that can be used. For example the Delete keyword can be abbreviated Del.

A command-line completion feature makes entering and repeating commands easier. Table B-1 describes the command-line completion keystrokes.

Table B-1. Command-Line Completion

Keystroke	Effect
Tab	Completes the command line. Enter at least one character and press the tab key to complete the command line. If more than one possibility exists, press the Tab key again to display all possibilities.
Up Arrow	Scrolls backward through the list of previously entered commands.
Down Arrow	Scrolls forward through the list of previously entered commands.
Control-A	Moves the cursor to the beginning of the command line
Control-E	Moves the cursor to the end of the command line.

B.3 Commands

The command set performs monitoring and configuration tasks. Commands related to monitoring tasks are available to all account names. Commands related to configuration tasks are available only within an admin session by accounts with Admin authority. An account must have Admin authority to enter the Admin Start command, which opens an admin session. Some configuration commands, such as the Security command, are available only to the Admin account name. Refer to the ”Admin Command” on page B-4.

The commands and their page numbers are listed in Table B-2.

Table B-2. Commands Listed by Authority Level

Monitoring Commands		Configuration Command	
Help	(B-17)	Admin	(B-4)
History	(B-19)	**Admin Session Commands**	
Ping	(B-24)		
Ps	(B-25)	Alias[1]	(B-5)
Quit	(B-26)	Config[1]	(B-7)
Show	(B-59)	Date[1]	(B-10)
Show Config	(B-72)	Fallback	(B-11)
Show Log	(B-75)	Group[1]	(B-12)
Show Perf	(B-77)	Hardreset	(B-16)
Show Setup	(B-79)	Hotreset	(B-20)
Uptime	(B-86)	Image	(B-21)
Whoami	(B-90)	Lip	(B-22)
		Passwd	(B-23)
		Reset	(B-27)
		Security	(B-32)
		Securityset[1]	(B-35)
		Set[1]	(B-37)
		Set Config	(B-39)
		Set Log	(B-50)
		Set Port	(B-53)
		Set Setup	(B-54)
		Shutdown	(B-82)
		Test	(B-83)
		User[1] [2]	(B-87)
		Zone[1]	(B-91)
		Zoneset[1]	(B-95)
		Zoning[1]	(B-97)

[1]Some keywords do not require an Admin session.

[2] Some keywords can be executed only by the Admin account name.

Admin Command

Opens and closes an Admin session. The Admin session provides commands that change the fabric and switch configurations. Only one Admin session can be open on the switch at any time. An inactive Admin session will time out after a period of time which can be changed using the Set Setup System command. Refer to the ”Set Setup Command” on page B-54.

Authority Admin

Syntax

admin
start (or begin)
end (or stop)
cancel

Keywords

start (or begin)
Opens the admin session.

end (or stop)
Closes the admin session. The Hardreset, Hotreset, Logout, Shutdown, and Reset Switch commands will also end an admin session.

cancel
Terminates an Admin session opened by another user. Use this keyword with care because it terminates the Admin session without warning the other user and without saving pending changes.

Notes Closing a Telnet window during an admin session does not release the session. In this case, you must either wait for the admin session to time out, or use the Admin Cancel command.

Examples The following example shows how to open and close an Admin session:

```
SANbox2 #> admin start

SANbox2 (admin) #>

.
.
.

SANbox2 (admin) #> admin end
```

Alias Command

Creates a named set of ports/devices. Aliases make it easier to assign a set of ports/devices to many zones. An alias can not have a zone or another alias as a member.

Authority Admin session for all keywords except List

Syntax **alias**

add [alias] [member_list]
copy [alias_source] [alias_destination]
create [alias]
delete [alias]
list
members [alias]
remove [alias] [member_list]
rename [alias_old] [alias_new]

Keywords

add [alias] [member_list]
Specifies one or more ports/devices given by [member_list] to add to the alias named [alias]. Use a <space> to delimit ports/devices in [member_list]. An alias can have a maximum of 2000 members. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs and port numbers are in decimal. Ports are numbered beginning with 0.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.

The application verifies that the [alias] format is correct, but does not validate that such a port/device exists.

copy [alias_source] [alias_destination]
Creates a new alias named [alias_destination] and copies the membership into it from the alias given by [alias_source].

create [alias]
Creates an alias with the name given by [alias]. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 256 aliases.

delete [alias]
Deletes the specified alias given by [alias] from the zoning database. If the alias is a member of the active zone set, the alias will not be removed from the active zone set until the active zone set is deactivated.

list
Displays a list of all aliases. This keyword does not require an admin session.

members [alias]
Displays all members of the alias given by [alias]. This keyword is available with User authority and does not require a zoning edit session or an admin session.

remove [alias] [member_list]
Removes the ports/devices given by [member_list] from the alias given by [alias]. Use a <space> to delimit ports/devices in [member_list]. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs and port numbers are in decimal. Ports are numbered beginning with 0.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) for the device with the format xx:xx:xx:xx:xx:xx:xx:xx.

rename [alias_old] [alias_new]
Renames the alias given by [alias_old] to the alias given by [alias_new].

Config Command

Manages the Fibre Channel configurations on a switch. For information about setting the port and switch configurations, refer to the ”Set Config Command” on page B-39.

Authority Admin session for all keywords except List

Syntax

config
activate *[config]*
backup
cancel
copy [config_source] [config_destination]
delete [config]
edit *[config]*
list
restore
save *[config]*

Keywords

activate *[config]*
Activates the configuration given by [config]. If you omit the configuration, the currently active configuration is used. Only one configuration can be active at a time.

backup
Creates a file named *configdata*, which contains the system configuration information. To download this file, open an FTP session, log in with account name/password of “images” for both, and type “get configdata”. Refer to Examples.

cancel
Terminates the current configuration edit session without saving changes that were made.

copy [config_source] [config_destination]
Copies the configuration given by [config_source] to the configuration given by [config_destination]. The switch supports up to 10 configurations including the default configuration.

delete [config]
Deletes the specified configuration file where [config] is a file name.

edit *[config]*
Opens an edit session for the configuration given by [config]. If you omit the configuration name, the currently active configuration is used.

list
Displays a list of all available configurations. This keyword is available with User authority.

restore
Restores configuration settings to an out-of-band switch from a backup file named *configdata*, which must be first uploaded on the switch using FTP. You create the backup file using the Config Backup command. Use FTP to load the backup file on a switch, then enter the Config Restore command. Refer to Examples.

Note:
- If the restore process changes the IP address, all management sessions are terminated. Use the Set Setup System command to return the IP configuration to the values you want. Refer to the "Set Setup Command" on page B-54.
- Configuration archive files created with the SANbox Manager Archive function are not compatible with the Config Restore command.

save *[config]*
Saves changes made during a configuration edit session in the configuration given by [config]. If you omit the configuration name value, the configuration you chose for the Config Edit command is used. The switch supports up to 10 configurations including the default configuration.

Notes

If you edit the active configuration, changes will be held in suspense until you reactivate the configuration or activate another configuration.

Examples

The following shows an example of how to open and close a Config Edit session:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
.
.
SANbox2 (admin-config) #> config cancel
  Configuration mode will be canceled. Please confirm (y/n): [n] y
SANbox2 (admin) #> admin end
```

The following is an example of how to create a backup file (configdata) and download the file to the workstation.

```
SANbox2 #> admin start
SANbox2 (admin) #> config backup
SANbox2 (admin) #> admin end
SANbox2 #> exit

#>ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> get configdata
ftp> quit
```

The following is an example of how to upload a configuration backup file (configdata) from the workstation to the switch, and then restore the configuration.

```
#> ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> put configdata
ftp> quit

SANbox2 #> admin start
SANbox2 (admin) #> config restore
The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
 Alarm Msg: [Tue Jun 10 09:25:56.938 2003][A1005.0021][SM][Configuration is being
restored -  this could take several minutes !]
  Alarm Msg: [Tue Jun 10 09:26:19.266 2003][A1000.000A][SM][The switch will be
reset in 3 seconds due to a config restore]
SANbox2 (admin) #>
  Alarm Msg: [Tue Jun 10 09:26:22.296 2003][A1000.0005][SM][The switch is being
reset]
Good bye.
```

Date Command

This command displays or sets the system date and time. To set the date and time the information string must be provided in this format: MMDDhhmmCCYY. The new date and time takes effect immediately.

Authority Admin session except to display the date.

Syntax **date**
[MMDDhhmmCCYY]

Keywords ***[MMDDhhmmCCYY]***
Specifies the date – this requires an admin session. If you omit [MMDDhhmmCCYY], the current date is displayed – this is available with User authority.

Examples The following is an example of the Date command:

```
SANbox2 #> date
  Mon Apr 07 07:51:24 2003
```

Fallback Command

Assigns the pending firmware status back and forth between the active and inactive firmware images stored in switch memory.

Authority Admin session

Syntax **fallback**

Notes

- The Show Switch command displays the two firmware images, active firmware, inactive firmware, and pending firmware versions.
- After executing the Fallback command, reset the switch to activate the pending firmware. Use the Hotreset command for a non-disruptive activation. Otherwise, you can use the Reset Switch command.

Examples The following is an example of the Fallback command:

```
SANbox2 #> admin start

SANbox2 (admin) #> fallback

  Reverting to previous software image.  Please confirm (y/n): [n] y
```

Group Command

Creates groups, manages membership within the group, and manages the membership of groups in security sets.

Authority Admin session and a Security Edit session. Refer to the "Security Command" on page B-32 for information about starting a Security Edit session. The List and Members keywords are available without an Admin session.

Syntax

group
add [group]
copy
create [group] *[type]*
delete [group]
edit [group] [member]
list
members [group]
rename [group_old] [group_new]

Keywords

add [group]
Initiates an editing session in which to specify a group member and its attributes for the group given by [group]. A group name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. Member attributes are described in Table B-3:

Table B-3. Group Member Attributes

Attribute	Description
Group Member	Switch worldwide name (ISL group) or the worldwide name of the N_Port device that would attach to the switch (Port and MS).
Authentication	Type of authentication to use: ■ None – no authentication ■ CHAP – Challenge Handshake Authentication Protocol (ISL and Port groups only) ■ MD5 – MD5 hash function (MS groups only) ■ SHA-1 – SHA-1 hash function (MS groups only)
Secret	16-byte (ISL and Port groups) or 20-byte (MS groups) hex string used for authentication purposes. Applies only for CHAP, MD5, and SHA-1 authentication.
DomainBinding	Binds the ISL group member worldwide name to the specified switch domain ID. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. Refer to the "Set Config Command" on page B-39. 0 (zero) specifies no binding.

copy [group_source] [group_destination]
Creates a new group named [group_destination] and copies the membership into it from the group given by [group_source].

create [group] ***[type]***
Creates a group with the name given by [group] with the type given by [type]. A group name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The security database supports a maximum of 16 groups. If you omit [type], ISL is used. [type] can be one of the following:

ISL
Configures security for attachments to other switches.

Port
Configures security for attachments to N_Port devices.

MS
Configures security for attachments to N_Port devices that are issuing management server commands.

edit [group] [member]
Initiates an editing session in which to change the attributes of a worldwide name given by [member] in a group given by [group]. Member attributes that can be changed are described in Table B-4:

Table B-4. Group Member Attributes

Attribute	Description
DomainBinding	Binds the ISL group member worldwide name to the specified switch domain ID. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. Refer to the "Set Config Command" on page B-39. 0 (zero) specifies no binding.
Authentication	Type of authentication to use: ■ None – no authentication ■ CHAP – Challenge Handshake Authentication Protocol (ISL and Port groups only) ■ MD5 – MD5 hash function (MS groups only) ■ SHA-1 – SHA-1 hash function (MS groups only)
Secret	16-byte (ISL and Port groups) or 20-byte (MS groups) hex string used for authentication purposes. Applies only for CHAP, MD5, and SHA-1 authentication.

list
Displays a list of all groups and the security sets of which they are members. This keyword is available without an Admin session.

members [group]
Displays all members of the group given by [group]. This keyword is available without an Admin session.

remove [group] [members]
Remove the port/device worldwide name given by [member] from the group given by [group].

rename [group_old] [group_new]
Renames the group given by [group_old] to the group given by [group_new].

Notes

Refer to the ”Securityset Command” on page B-35 for information about managing groups in security sets.

Examples

The following is an example of the Group Add command:

```
SANbox2 (admin-security) #> group add Group_1
Group Type is ISL
Group Member (wwn)              [00:00:00:00:00:00:00:00 ] 10:00:00:c0:dd:00:90:a4
Authentication (None/Chap)       [None ] Chap
Secret (16 byte hex value)       [0 ] 12345678123456781234567812345678
```

The following is an example of the Group Edit command:

```
SANbox2 (admin-security) #> group edit G1 10:00:00:c0:dd:00:90:a3
A list of attributes with formatting and default values will follow
Enter a new value or simply press the ENTER key to accept the current value
with exception of the Group Member WWN field which is mandatory.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.
Group Type : ISL
Group Member: 10:00:00:c0:dd:00:90:a3
Authentication (None / Chap)     [None]
Secret  (32-character hex value   [    ]
Finished configuring attributes.
To discard this configuration use the security cancel command.
```

The following is an example of the Group List command:

```
SANbox2 #> group list
  Group       SecuritySet
  -----       -----------
  group1 (ISL)
              alpha
  group2 (Port)
              alpha
```

The following is an example of the Group Members command:

```
SANbox2 #> group members group1
  Current list of members for Group: group1
  ---------------------------------
  10:00:00:c0:dd:00:71:ed
  10:00:00:c0:dd:00:72:45
  10:00:00:c0:dd:00:90:ef
  10:00:00:c0:dd:00:b8:b7
```

Hardreset Command

Resets the switch and performs a power-on self test. This reset activates the pending firmware and disrupts traffic.

Authority Admin session

Syntax **hardreset**

Notes To reset the switch without a power-on self test, refer to the ”Reset Command” on page B-27.

To reset the switch without disrupting traffic, refer to the ”Hotreset Command” on page B-20.

Help Command

Displays a brief description of the specified command and its keywords.

Authority None

Syntax **help *[command] [keyword]***

Keywords ***[command]***
Displays a summary of the command given by [command] and its keywords. If you omit [command], the system displays all available commands from which to choose.

[keyword]
Displays a summary of the keyword given by [keyword] belonging to the command given by [command]. If you omit [keyword], the system displays the available keywords for the specified command.

all
Displays a list of all available commands (including command variations).

Examples The following is an example of the Help Set command:

```
SANbox2 #> help set

set SET_OPTIONS
There are many attributes that can be set.
Type help with one of the following to get more information:
    set alarm
    set beacon
    set blade
    set config blade
    set config port
    set config ports
    set config security
    set config switch
    set config threshold
    set config zoning
    set log
    set pagebreak
    set port
    set setup snmp
    set setup system
    set switch
```

The following is an example of the Help Set Beacon command:

```
SANbox2 #> help set beacon
set beacon On | Off
This command allows the LEDs on the front of the switch to flash.
The On option will start and the Off option will stop the flashing.
```

History Command

Displays a numbered list of the previously entered commands from which you can re-execute selected commands.

Authority None

Syntax **history**

Notes Use the History command to provide context for the ! command:

- Enter ![command] to re-enter the most recent execution of that command.
- Enter ![line number] to re-execute the corresponding command from the History display
- Enter ![partial command string] to re-execute a command that matches the command string.
- Enter !! to re-execute the most recent command.

Examples The following is an example of the History command:

```
SANbox2 #> history
   1 show switch
   2 date
   3 help set
   4 history

SANbox2 #> !3
help set

set SET_OPTIONS
There are many attributes that can be set.
Type help with one of the following to get more information:
    set alarm
    set beacon
    set blade
    set config blade
    set config port
    set config ports
    set config switch
    set config threshold
    set config zoning
    set log
    set pagebreak
    set port
    set setup snmp
    set setup system
    set switch
```

Hotreset Command

Resets the switch for the purpose of activating the pending firmware without disrupting traffic. This command terminates all management sessions and saves all configuration information. After the pending firmware is activated, the configuration is recovered. This process takes less than 80 seconds.

Authority Admin session

Syntax **hotreset**

Notes Non-disruptive firmware activation is possible under the following conditions:

- The active firmware must be version 2.0 or greater and the new firmware to be activated must be a version greater than 2.0.
- The fabric must be stable. This means that no configuration changes can be in progress, and switch and device connections are not being added or removed. Furthermore, a non-disruptive activation cannot occur if any port in the fabric is in the diagnostic operational state.

This command clears the event log and all counters.

Image Command

Manages and installs switch firmware.

Authority Admin session

Syntax

image
cleanup
fetch [account_name] [ip_address] [file_source] [file_destination]
list
unpack [file]

Keywords

cleanup
Removes all firmware image files from the switch. All firmware image files are removed automatically each time the switch is reset.

fetch [account_name] [ip_address] [file_source] [file_destination]
Retrieves image file given by [file_source] and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the device with the IP address given by [ip_address] and an account name given by [account_name]. If an account name needs a password to access the device, the system will prompt you for it.

list
Displays the list of image files that reside on the switch.

unpack [file]
Installs the firmware file given by [file]. After unpacking the file, a message appears confirming successful unpacking. The switch must be reset for the new firmware to take effect.

Notes To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

Use the Hotreset command to perform a non-disruptive activation for firmware versions that follow version 2.0.

Lip Command

Reinitializes the specified loop port.

Authority Admin session

Syntax **lip [port_number]**

Keywords **[port_number]**
The number of the port to be reinitialized.

Examples The following is an example of the Lip command:

```
SANbox2 (admin) #> lip 2
```

Passwd Command

Changes a user account's password.

Authority Admin account name and an admin session to change another account's password; You can change you own password without an Admin session.

Syntax **passwd [account_name]**

Keywords **[account_name]**
The user account name. To change the password for an account name other than your own, you must open an admin session with the account name Admin. If you omit [account_name], you will be prompted to change the password for the current account name.

Examples The following is an example of the Passwd command:

```
SANbox2 (admin) #> passwd user2

     Press 'q' and the ENTER key to abort this command.

  account OLD password               :
  account NEW password (4-20 chars)  :

  please confirm account NEW password:
  password has been changed.
```

Ping Command

Initiates an attempt to communicate with another switch in the fabric and reports the result.

Authority None

Syntax **Ping**
ip_address

Keywords **ip_address**
The IP address of the switch to query.

Examples The following is an example of a successful Ping command:

```
SANbox2 #> ping 10.20.11.57
  Ping command issued. Waiting for response...
SANbox2 #>
  Response successfully received from 10.20.11.57.
```

This following is an example of an unsuccessful Ping command:

```
SANbox2 #> ping 10.20.10.100
  Ping command issued. Waiting for response...
  No response from 10.20.10.100. Unreachable.
```

Ps Command

Displays current system process information.

Authority None

Syntax **ps**

Examples The following is an example of the Ps command:

```
SANbox2 #> ps
PID  PPID %CPU     TIME     ELAPSED COMMAND
338   327  0.0 00:00:00  3-01:18:35 cns
339   327  0.0 00:00:01  3-01:18:35 ens
340   327  0.0 00:00:21  3-01:18:35 dlog
341   327  0.1 00:05:35  3-01:18:35 ds
342   327  0.2 00:11:29  3-01:18:35 mgmtApp
343   327  0.0 00:00:04  3-01:18:35 fc2
344   327  0.0 00:02:16  3-01:18:35 nserver
345   327  0.0 00:02:44  3-01:18:35 mserver
346   327  0.8 00:35:12  3-01:18:35 util
347   327  0.0 00:00:29  3-01:18:35 snmpservicepath
348   327  0.0 00:02:46  3-01:18:34 eport
349   327  0.0 00:00:21  3-01:18:34 PortApp
350   327  5.6 04:08:24  3-01:18:34 port_mon
351   327  0.0 00:01:38  3-01:18:34 zoning
352   327  0.0 00:00:01  3-01:18:34 diagApp
404   327  0.0 00:00:04  3-01:18:27 snmpd
405   327  0.0 00:00:02  3-01:18:27 snmpmain
406   405  0.0 00:00:00  3-01:18:26 snmpmain
```

Quit Command

Closes the Telnet session.

Authority None

Syntax **quit, exit, or logout**

Notes You can also enter Control-D to close the Telnet session.

Reset Command

Resets the switch configuration parameters. If you omit the keyword, the default is Reset Switch.

Authority Admin session

Syntax **reset**

config *[config_name]*
factory
port [port_number]
security
snmp
switch (default)
system
zoning

Keywords **config *[config_name]***

Resets the configuration given by [config_name] to the factory default values for switch, port, alarm threshold, and zoning configuration. If [config_name] does not exist on the switch, a configuration with that name will be created. If you omit [config_name], the active configuration is reset. You must activate the configuration for the changes to take effect. Refer to Table B-5 through Table B-8 for switch, port, and alarm threshold configuration default values.

factory

Resets switch configuration, port configuration, alarm threshold configuration, zoning configuration, SNMP configuration, system configuration, security configuration, and zoning to the factory default values. The switch configuration is activated automatically. Refer to Table B-5 through Table B-10.

port [port_number]

Reinitializes the port given by [port_number]. Ports are numbered beginning with 0.

security

Clears the security database and deactivates the active security set. The security configuration value, autosave, and fabric binding remain unchanged. Refer to Table B-11 for security configuration default values.

snmp

Resets the SNMP configuration settings to the factory default values. Refer to Table B-9 for SNMP configuration default values.

switch

Resets the switch without a power-on self test. This reset disrupts traffic and activates the pending firmware. This command also closes all management sessions. This is the default. To reset the switch with a power-on self test, refer to the ”Hardreset Command” on page B-16. To reset the switch without disrupting traffic, refer to the ”Hotreset Command” on page B-20.

system
Resets the system configuration settings to the factory default values. Refer to Table B-10 for system configuration default values.

zoning
Clears the zoning database and deactivates the active zone set. The zoning configuration values (autosave, default visibility) remain unchanged.

Notes

The following tables specify the various factory default settings:

Table B-5. Switch Configuration Defaults

Parameter	Default
Admin State	Online
Broadcast Enabled	True
InbandEnabled	True
FDMIEnabled	True
FDMIEntries	1000
Domain ID	1 (0x Hex)
Domain ID Lock	False
Symbolic Name	SANbox2
R_A_TOV	10000
E_D_TOV	2000
Principal Priority	254
Configuration Description	QLogic SANbox2 FC Switch

Table B-6. Port Configuration Defaults

Parameter	Default
Admin State	Online
Link Speed	Auto
Port Type	GL
Symbolic Name	Port
ALFairness	False
DeviceScanEnabled	True
ForceOfflineRSCN	False

Table B-6. Port Configuration Defaults (Continued)

Parameter	Default
ARB_FF	False
InteropCredit	0
ExtCredit	0
FANEnable	True
LCFEnable	False
MFSEnable	True
MFS_TOV	10
MSEnable	True
NoClose	False
IOStreamGuard	Disabled
VIEnable	False

Table B-7. Alarm Threshold Configuration Defaults

Parameter	Default
ThresholdMonitoringEnabled	False
CRCErrorsMonitoringEnabled	True
RisingTrigger	25
FallingTrigger	1
SampleWindow	10
DecodeErrorsMonitoringEnabled	True
RisingTrigger	200
FallingTrigger	0
SampleWindow	10
ISLMonitoringEnabled	True
RisingTrigger	2
FallingTrigger	0
SampleWindow	10
LoginMonitoringEnabled	True
RisingTrigger	5
FallingTrigger	1
SampleWindow	10

Table B-7. Alarm Threshold Configuration Defaults (Continued)

Parameter	Default
LogoutMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 5 1 10
LOSMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 100 5 10

Table B-8. Zoning Configuration Defaults

Parameter	Default
FC-SW-2 AutoSave	True
Default Visibility	All

Table B-9. SNMP Configuration Defaults

Parameter	Default
SNMPEnabled	True
Contact	<syscontact undefined>
Location	<sysLocation undefined>
Description	QLogic SANbox2 FC Switch
Trap [1-5] Address	Trap 1: 10.0.0.254; Traps 2–5: 0.0.0.0
Trap [1-5] Port	162
Trap [1-5] Severity	Warning
Trap [1-5] Version	2
Trap [1-5] Enabled	False
ObjectID	1.3.6.1.4.1.1663.1.1.1.1.11
AuthFailureTrap	False
ProxyEnabled	True

Table B-10. System Configuration Defaults

Parameter	Default
Ethernet Network Discovery	Static
Ethernet Network IP Address	10.0.0.1
Ethernet Network IP Mask	255.0.0.0
Ethernet Gateway Address	10.0.0.254
Fibre Channel Network Discovery	Static
Fibre Channel Network IP Address	0.0.0.0
Fibre Channel Network IP Mask	255.0.0.0
Fibre Channel Gateway Address	10.0.0.254
Admin Timeout	30 minutes
UserAuthentication	False
LocalLogEnabled	True
RemotelogEnabled	False
RemoteLogHostAddress	10.0.0.254
Temp Monitoring Warning	65
Temp Monitoring Failure	70
Temp Failure Port Shutdown	False

Table B-11. Security Configuration Defaults

Parameter	Default
AutoSave	True
FabricBindingEnabled	True

Security Command

Opens a Security Edit session in which to manage the security database on a switch. Refer to the ”Group Command” on page B-12 and the ”Securityset Command” on page B-35.

Authority Admin session. The keywords Active, History, Limits, and List are available without an Admin session.

Syntax

security
- active
- cancel
- clear
- edit
- history
- limits
- list
- restore
- save

Keywords

active
Displays the active security set, its groups, and group members. This keyword does not require an Admin session.

cancel
Closes a Security Edit session without saving changes. Use the Edit keyword to open a Security Edit session.

clear
Clears all inactive security sets from the volatile edit copy of the security database. This keyword does not affect the non-volatile security database. However, if you enter the Security Clear command followed by the Security Save command, the non-volatile security database will be cleared from the switch.

Note: The preferred method for clearing the security database from the switch is the Reset Security command. Refer to the ”Reset Command” on page B-27.

edit
Initiates a Security Edit session in which to make changes to the security database. A Security Edit session enables you to use the Group and Securityset commands to create, add, and delete security sets, groups, and group members. To close a Security Edit session and save changes, enter the Security Save command. To close a Security Edit session without saving changes, enter the Security Cancel command.

history
Displays history information about the security database and the active security set including the account name that made changes and when those changes were made. This keyword does not require an Admin session.

limits
Displays the current totals and the security database limits for the number of security sets, groups, members per group, and total members. This keyword does not require an Admin session.

list
Displays all security sets, groups, and group members in the security database. This keyword does not require an Admin session.

restore
Reverts the changes to the security database that have been made during the current Security Edit session since the last Security Save command was entered.

save
Saves the changes that have been made to the security database during a Security Edit session. Changes you make to any security set will not take effect until you activate that security set. Refer to the ”Securityset Command” on page B-35 for information about activating a security set.

Examples

The following is an example of the Security Active command:

```
SANbox2 #> security active
  Active Security Information

  SecuritySet  Group  GroupMember             Auth   Secret
  -----------  -----  -----------             ----   ------
  No active securitysets defined.
```

The following is an example of the Security History command:

```
SB211.192 #> security history
  Active Database Information
  ---------------------------
  SecuritySetLastActivated/DeactivatedBy  Remote
  SecuritySetLastActivated/DeactivatedOn  Wed Aug 13 12:21:40 2003
  Database Checksum                   00000000

  Inactive Database Information
  -----------------------------
  ConfigurationLastEditedBy           admin@IB-session11
  ConfigurationLastEditedOn           Tue Aug 12 12:18:37 2003
  Database Checksum                   00007558
```

The following is an example of the Security Limits command:

```
SANbox2 #> security limits
  Security Attribute   Maximum   Current   [Name]
  ------------------   -------   -------   ------
  MaxSecuritySets      4         1
  MaxGroups            16        2
  MaxTotalMembers      1000      19
  MaxMembersPerGroup   1000
                                 4         group1
                                 15        group2
```

The following is an example of the Security List command:

```
SANbox2 (admin-security) #> security list
SB211.192 #> security list
  Active Security Information
  SecuritySet  Group  GroupMember              Auth   Secret
  -----------  -----  -----------              ----   ------
  No active securityset defined.

  Configured Security Information
  SecuritySet  Group  GroupMember              Auth   Secret
  -----------  -----  -----------              ----   ------
  alpha
               group1 (ISL)
                      10:00:00:c0:dd:00:71:ed  None
                      10:00:00:c0:dd:00:72:45  None
                      10:00:00:c0:dd:00:90:ef  None
                      10:00:00:c0:dd:00:b8:b7  None

               group2 (Port)
                      21:00:00:20:37:19:16:55  None
                      21:00:00:20:37:19:1f:b0  None
                      21:00:00:20:37:19:2c:71  None
                      21:00:00:20:37:19:31:0d  None
                      21:00:00:20:37:19:31:2b  None
                      21:00:00:20:37:19:31:7b  None
                      21:00:00:20:37:19:31:bd  None
                      21:00:00:e0:8b:07:ae:bc  None
                      21:00:00:e0:8b:09:3b:17  None
                      22:00:00:04:cf:28:b2:ad  None
                      22:00:00:04:cf:4a:67:ff  None
                      22:00:00:04:cf:4a:77:dd  None
```

Securityset Command

Manages security sets in the security database.

Authority Admin session and a Security Edit session. Refer to the "Security Command" on page B-32 for information about starting a Security Edit session. The Active, Groups, and List keywords are available without an Admin session. You must close the Security Edit session before using the Activate and Deactivate keywords.

Syntax

securityset
activate [security_set]
active
add [security_set] [group_list]
copy [security_set_source] [security_set_destination]
create [security_set]
deactivate
delete [security_set]
groups [security_set]
list
remove [security_set] [group]
rename [security_set_old] [security_set_new]

Keywords

activate [security_set]
Activates the security set given by [security_set]. This keyword deactivates the active security set. Close the Security Edit session using the Security Save or Security Cancel command before using this keyword.

active
Displays the name of the active security set. This keyword is available without an Admin session.

add [security_set] [group_list]
Adds one or more groups given by [group_list] to the security set given by [security_set]. Use a <space> to delimit multiple group names in [group_list]. A security set can have a maximum of three groups with no more than one group of each group type.

copy [security_set_source] [security_set_destination]
Creates a new security set named [security_set_destination] and copies into it the membership from the security set given by [security_set_source].

create [security_set]
Creates the security set with the name given by [security_set]. A security set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The security database supports a maximum of 4 security sets.

deactivate
Deactivates the active security set. Close the Security Edit session before using this keyword.

delete [security_set]
Deletes the security set given by [security_set]. If the specified security set is active, the command is suspended until the security set is deactivated.

groups [security_set]
Displays all groups that are members of the security set given by [security_set]. This keyword is available without an Admin session.

list
Displays a list of all security sets. This keyword is available without an Admin session.

remove [security_set] [group]
Removes a group given by [group] from the security set given by [security_set]. If [security_set] is the active security set, the group will not be removed until the security set has been deactivated.

rename [security_set_old] [security_set_new]
Renames the security set given by [security_set_old] to the name given by [security_set_new].

Notes

Refer to the ”Group Command” on page B-12 for information about creating and managing groups.

Examples

The following is an example of the Securityset Active command

```
SANbox2 #> securityset active
  Active SecuritySet Information
  ------------------------------
  ActiveSecuritySet -- none --
  LastActivatedBy  Remote
  LastActivatedOn  Wed Aug 13 12:21:40 2003
```

The following is an example of the Securityset Groups command

```
SANbox2 #> securityset groups alpha
  Current list of Groups for SecuritySet: alpha
  --------------------------------------
  group1 (ISL)
  group2 (Port)
```

The following is an example of the Securityset List command

```
SANbox2 #> securityset list
  Current list of SecuritySets
  ----------------------------
  alpha
  beta
```

Set Command

Sets a variety of switch parameters.

Authority Admin session for all keywords except Alarm Clear, Beacon, and Pagebreak which are available without an Admin session.

Syntax

set
alarm clear
beacon [state]
config [option]
log [option]
pagebreak [state]
port [option]
setup [option]
switch [state]

Keywords

alarm clear
Clears the alarm log. This keyword is available with User authority.

beacon [state]
Enables or disables the flashing of the Logged-In LEDs according to [state]. This keyword is available with User authority. [state] can be one of the following:

on
Enables the flashing beacon.

off
Disables the flashing beacon.

config [option]
Sets switch, port, alarm threshold, and zoning configuration parameters. Refer to the ”Set Config Command” on page B-39.

log [option]
Specifies the type of entries to be entered in the event log. Refer to the ”Set Log Command” on page B-50.

pagebreak [state]
Specifies how much information is displayed on the screen at a time according to the value given by [state]. This keyword is available with User authority. [state] can be one of the following:

on
Limits the display of information to 20 lines at a time. The page break functions affects the following commands: Alias (List, Members), Show (Alarm, Log), Zone (List, Members), Zoneset (List, Zones), Zoning (Active, List).

off
Allows continuous display of information without a break.

port [option]
Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. Refer to the ”Set Port Command” on page B-53.

setup [option]
Changes SNMP and system configuration settings. Refer to the ”Set Setup Command” on page B-54.

switch [state]
Temporarily changes the administrative state for all ports on the switch to the state given by [state]. The previous Set Config Switch settings are restored after a switch reset or a reactivation of a switch configuration. [state] can be one of the following:

online
Places all ports online

offline
Places all ports offline.

diagnostics
Prepares all ports for testing.

Examples

The following examples enables and disables the beacon:

```
SANbox2 #> set beacon on

  Command succeeded.

SANbox2 $> set beacon off

  Command succeeded.
```

Set Config Command

Sets switch, port, alarm threshold, security, and zoning configuration parameters.

Authority Admin session and a Config Edit session

Syntax

set config
port *[port_number]*
ports *[port_number]*
security
switch
threshold
zoning

Keywords

port *[port_number]*
Initiates an edit session in which to change configuration parameters for the port number given by [port_number]. If you omit [port_number], the system begins with port 0 and proceeds in order through the last port. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” to end the configuration for one port, or “qq” to end the configuration for all ports. Table B-12 describes the port parameters.

ports *[port_number]*
Initiates an editing session in which to change configuration parameters for all ports based on the configuration for the port given by [port_number]. If you omit [port_number], port 0 is used. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” to end the configuration. Table B-12 describes the port parameters.

Table B-12. Set Config Port Parameters

Parameter	Description
AdminState	Port administrative state: online, offline, diagnostics, or down. The default is online.
LinkSpeed	Transmission speed: 1Gb/sec, 2 Gb/sec, or Auto. The default is Auto.
PortType	Port mode: GL, G, F, FL, Donor. The default is GL.
SymbolicPortName	Descriptive name. The default is Port.
ALFairness	Arbitration loop fairness. Enables (True) or disables (False) the switch’s priority to arbitrate on the loop. The default is False.

Table B-12. Set Config Port Parameters (Continued)

Parameter	Description
DeviceScanEnabled	Enables (True) or disables (False) the scanning of the connected device for FC-4 descriptor information during login. The default is True.
ForceOfflineRSCN	Enables (False) or disables (True) the immediate transmission of RSCN messages when communication between a port and its device is interrupted. If enabled, the RSCN message is queued for 200 ms. The default is False. This parameter is ignored if IOStreamGuard is enabled.
ARB_FF	Send ARB_FF (True) instead of IDLEs (False) on the loop. The default is False.
InteropCredit	Interoperability credit. The number of buffer-to-buffer credits per port. 0 means the default (12) is unchanged.
ExtCredit	Extended credits. The number of port buffer credits that this port can acquire from donor ports. The default is 0.
FANEnable	Fabric address notification. Enables (True) or disables (False) the communication of the FL_Port address, port name, and node name to the logged-in NL_Port. The default is True.
LCFEnable	Link control frame preference routing. Enables (True) or disables (False) preferred routing of frames with R_CTL = 1100 (Class 2 responses). The default is False. Enabling LCFEnable will disable MFSEnable.
MFSEnable	Multi-Frame Sequence bundling. Prevents (True) or allows (False) the interleaving of frames in a sequence. The default is True. Enabling MFSEnable disables LCFEnable and VIEnable.

Table B-12. Set Config Port Parameters (Continued)

Parameter	Description
MSEnable	Management server enable. Enables (True) or disables (False) management server on this port. The default is True.
NoClose	Loop circuit closure prevention. Enables (True) or disables (False) the loop's ability to remain in the open state indefinitely. True reduces the amount of arbitration on a loop when there is only one device on the loop. The default is False.
IOStreamGuard	I/O Stream Guard. Enable (Enable) or disables (Disable) the suppression of RSCN messages. The default is Disable.
VIEnable	Enables (True) or disables (False) VI preference routing. The default is False. Enabling VIEnable will disable MFSEnable.

security
Initiates an editing session in which to change the security settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” or "Q" to end the editing session. Table B-13 describes the Set Config Security parameters.

Table B-13. Security Configuration Parameters

Parameter	Description
AutoSave	Enables (True) or disables (False) the propagation of the active security set to all switches in the fabric. The default is True.
FabricBindingEnabled	Enables (True) or disables (False) the configuration and enforcement of fabric binding. Fabric binding associates switch worldwide names with a domain ID in the creation of ISL groups.

switch
Initiates an editing session in which to change switch configuration settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Table B-14 describes the Set Config Switch parameters.

Table B-14. Set Config Switch Parameters

Parameter	Description
AdminState	Switch administrative state: online, offline, or diagnostics. The default is Online.
BroadcastEnabled	Broadcast. Enables (True) or disables (False) forwarding of broadcast frames. The default is True.
InbandEnabled	Inband management. Enables (True) or disables (False) the ability to manage the switch over an ISL. The default is True.
FDMIEnabled	Fabric Device Monitoring Interface. Enables (True) or disables (False) the monitoring of target and initiator device information.
FDMIEntries	The number of device entries to maintain in the FDMI database. Enter a number from 0–1000. The default is 1000.
DefaultDomainID	Default domain ID. The default is 1.
DomainIDLock	Prevents (True) or allows (False) dynamic reassignment of the domain ID. The default is False.
SymbolicName	Descriptive name. The default is SANbox2.
R_A_TOV	Resource Allocation Timeout Value. The number of milliseconds the switch waits to allow two ports to allocate enough resources to establish a link. The default is 10000.
E_D_TOV	Error Detect Timeout Value. The number of milliseconds a port is to wait for errors to clear. The default is 2000.

Table B-14. Set Config Switch Parameters (Continued)

Parameter	Description
PrincipalPriority	The priority used in the FC-SW-2 principal switch selection algorithm. 1 is high, 255 is low. The default is 254.
ConfigDescription	The name for the configuration. The default is undefined.
FC-SW-2 Compliant	Propagates just the active zone set throughout the fabric (True, compliant) or the entire zoning database (False, non-compliant). The default is True.
LegacyAddressFormat	Available only when the FC-SW-2 Compliant parameter is False, this parameter enables (True) or disables (False) the use of legacy address formatting for interoperating with non-FC-SW-2 switches. Refer to ”FC-SW-2 Compliant” on page B-43. The default is False.

threshold

Initiates a configuration session by which to generate and log alarms for selected events. The system displays each event, its thresholds, and sampling interval one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. These parameters must be saved in a configuration and activated before they will take effect. Refer to the ”Config Command” on page B-7 for information about saving and activating a configuration. Table B-15 describes the Set Config Threshold parameters. The switch will down a port if an alarm condition is not cleared within three consecutive sampling intervals (by default 30 seconds). Reset the port to bring it back online. An alarm is cleared when the threshold monitoring detects that the error rate has fallen below the falling threshold.

Table B-15. Set Config Threshold Parameters

Parameter	Description
Threshold Monitoring Enabled	Master enable/disable parameter for all events. Enables (True) or disables (False) the generation of all enabled event alarms. The default is False.
CRCErrorsMonitoringEnabled DecodeErrorsMonitoringEnabled ISLMonitoringEnabled LoginMonitoringEnabled LogoutMonitoringEnabled LOSMonitoringEnabled	The event type enable/disable parameter. Enables (True) or disables (False) the generation of alarms for each of the following events: ■ CRC errors ■ Decode errors ■ ISL connection count ■ Device login errors ■ Device logout errors ■ Loss-of-signal errors
Rising Trigger	The event count above which a rising threshold alarm is logged. The switch will not generate another rising threshold alarm for that event until the count descends below the falling threshold and again exceeds the rising threshold.
Falling Trigger	The event count below which a falling threshold alarm is logged. The switch will not generate another falling threshold alarm for that event until the count exceeds the rising threshold and descends again below the falling threshold.
Sample Window	The period of time in seconds in which to count events.

zoning
Initiates an editing session in which to change switch zoning attributes. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table B-16. Set Config Zoning Parameters

Parameter	Description
FC-SW-2 AutoSave	Available only when the FC-SW-2 Compliant parameter is True, this parameter enables (True) or disables (False) the saving of changes to active zone set in the switch's permanent memory. Refer to "FC-SW-2 Compliant" on page B-43. The default is True.
Default Visibility	Enables (All) or disables (None) communication among the switch's ports/devices and the fabric in the absence of an active zone set. The default is All.

Examples

The following is an example of the Set Config Port command:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
SANbox2 (admin-config) #> set config port 1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  1
  ------------------------

  AdminState    (1=Online, 2=Offline, 3=Diagnostics, 4=Down)       [Online]
  LinkSpeed     (1=1Gb/s, 2=2Gb/s, 3=Auto)                         [Auto  ]
  PortType      (GL / G / F / FL / Donor)                          [GL    ]
  SymPortName   (string, max=32 chars)                             [Port1 ]
  ALFairness    (True / False)                                     [False ]
  DeviceScanEnable (True / False)                                  [True    ]
  ForceOfflineRSCN (True / False)                                  [False   ]
  ARB_FF        (True / False)                                     [False ]
```

```
  InteropCredit (decimal value, 0-255)                          [0     ]
  ExtCredit     (dec value, increments of 11, non-loop only)    [0     ]
  FANEnable     (True / False)                                  [True  ]
  LCFEnable     (True / False)                                  [False ]
  MFSEnable     (True / False)                                  [False ]
  MSEnable      (True / False)                                  [True  ]
  NoClose       (True / False)                                  [False ]
  IOStreamGuard (Enable / Disable)                              [Disable]
  VIEnable      (True / False)                                  [False ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Security command:

```
SANbox2 (admin-config) #> set config security
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  AutoSave            (True / False)     [True]

 Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Switch command:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
SANbox2 (admin-config) #> set config switch

  A list of attributes with formatting and default values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  AdminState         (1=Online, 2=Offline, 3=Diagnostics) [Online       ]
  BroadcastEnable    (True / False)                       [False        ]
  InbandEnabled      (True / False)                       [False        ]
  FDMIEnabled        (True / False)                       [True         ]
  FDMIEntries        (decimal value, 0-1000)              [1000         ]
  DefaultDomainID    (decimal value, 1-239)               [11           ]
  DomainIDLock       (True / False)                       [True         ]
  SymbolicName       (string, max=32 chars)               [SANbox2 switch]
  R_A_TOV            (decimal value, 100-100000 msec)     [10000        ]
  E_D_TOV            (decimal value, 10-20000 msec)       [2000         ]
  PrincipalPriority  (decimal value, 1-255)               [254          ]
  ConfigDescription  (string, max=32 chars)               [             ]
  FC-SW-2 Compliant  (True / False)                       [True         ]
```

The following is an example of the Set Config Threshold command:

```
SANbox2 #> admin start
SANbox2  (admin) #> config edit
SANbox2 (admin-config) #> set config threshold

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

ThresholdMonitoringEnabled     (True / False)              [False]

CRCErrorsMonitoringEnabled     (True / False)              [True]
  RisingTrigger                (decimal value, 1-1000)     [25 ]
  FallingTrigger               (decimal value, 0-1000)     [1 ]
  SampleWindow                 (decimal value, 1-1000 sec) [10 ]

DecodeErrorsMonitoringEnabled  (True / False)              [True]
```

```
  RisingTrigger              (decimal value, 1-1000)     [200 ]
  FallingTrigger             (decimal value, 0-1000)     [0 ]
  SampleWindow               (decimal value, 1-1000 sec) [10 ]

ISLMonitoringEnabled         (True / False)              [True]
  RisingTrigger              (decimal value, 1-1000)     [2 ]
  FallingTrigger             (decimal value, 0-1000)     [0 ]
  SampleWindow               (decimal value, 1-1000 sec) [10 ]

LoginMonitoringEnabled       (True / False)              [True]
  RisingTrigger              (decimal value, 1-1000)     [5 ]
  FallingTrigger             (decimal value, 0-1000)     [1 ]
  SampleWindow               (decimal value, 1-1000 sec) [10 ]

LogoutMonitoringEnabled      (True / False)              [True]
  RisingTrigger              (decimal value, 1-1000)     [5 ]
  FallingTrigger             (decimal value, 0-1000)     [1 ]
  SampleWindow               (decimal value, 1-1000 sec) [10 ]

LOSMonitoringEnabled         (True / False)               [True]
  RisingTrigger              (decimal value, 1-1000)     [100 ]
  FallingTrigger             (decimal value, 0-1000)     [5 ]
  SampleWindow               (decimal value, 1-1000 sec)  [10 ]

Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Zoning command.

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
SANbox2 (admin-config) #> set config zoning

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.

  FC-SW-2 AutoSave     (True / False)  [True]
  Default Visibility   (All / None)    [All ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

Set Log Command

Specifies the type of entries to be entered in the event log. Log entries are created for ports, components, and event severity levels.

Authority Admin session

Syntax **set log**
archive
clear
component [list]
level [level]
port [port_list]
restore
save
start (default)
stop

Keywords **archive**
Collects the most recent 200 entries plus the previous 1000 entries and stores the result in new file named *logfile* that is maintained in switch memory where it can be downloaded using FTP. To download *logfile*, open an FTP session, log in with account name/password of “images” for both, and type “get logfile”.

clear
Clears all log entries.

component [list]
Specifies one or more components to monitor for events. Use <space> to delimit values in the list. Choose one or more of the following values:

All
Monitors all components. To maintain optimal switch performance, do not use this setting with the Level keyword set to Info.

Chassis
Monitors chassis hardware components such as fans and power supplies.

Eport
Monitors all E_Ports.

Mgmtserver
Monitors management server status.

Nameserver
Monitors name server status.

None
Monitor none of the component events.

Other
Monitors other miscellaneous events.

Port
Monitors all port events

Switch
Monitors switch management events.

Zoning
Monitors zoning conflict events.

level [level]
Specifies the severity level given by [level] to use in monitoring events for the specified components or ports. [level] can be one of the following values:

Critical
Monitors critical events.

Warn
Monitors warning events.

Info
Monitors informational events. To maintain optimal switch performance, do not use this setting with the Component keyword set to All.

None
Monitors none of the severity levels.

port [port_list]
Specifies one or more ports to monitor for events. Choose one of the following values:

[port_list]
Specifies port or ports to monitor. Use a <space> to delimit values in the list. Ports are numbered beginning with 0.

All
Specifies all ports.

None
Disables monitoring on all ports.

restore
Restores and saves the port, component, and level settings to the default values.

save
Saves the log settings for the component, level, and port. These settings remain in effect after a switch reset. The log settings can be viewed using the Show Log Settings command. To export log entries to a file, use the Set Log Archive command.

start
Starts the logging of events based on the Port, Component, and Level keywords assigned to the current configuration. The logging continues until you enter the Set Log Stop command.

stop
Stops logging of events.

Notes To maintain optimal switch performance, do not set the Component keyword to All and the Level keyword to Info at the same time.

Set Port Command

Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. This command also clears port counters.

Authority Admin session

Syntax

set port [port_number]
bypass [alpa]
clear
enable
speed [transmission_speed]
state [state]

Keywords

[port_number]
Specifies the port. Ports are numbered beginning with 0.

bypass [alpa]
Sends a Loop Port Bypass (LPB) to a specific Arbitrated Loop Physical Address (ALPA) or to all ALPAs on the arbitrated loop. [alpa] can be a specific ALPA or the keyword ALL to choose all ALPAs.

clear
Clears the counters on the specified port.

enable
Sends a Loop Port Enable (LPE) to all ALPAs on the arbitrated loop.

speed [transmission_speed]
Specifies the transmission speed for the specified port. Choose one of the following port speed values:

1Gb/s
One gigabit per second.

2Gb/s
Two gigabits per second.

Auto
The port speed is automatically detected.

state [state]
Specifies one of the following administrative states for the specified port:

Online
Places the port online.

Offline
Places the port offline.

Diagnostics
Prepares the port for testing.

Down
Disables the port.

Set Setup Command

Changes SNMP and system configuration settings. The switch maintains one SNMP configuration and one system configuration.

Authority Admin session

Syntax **set setup**
snmp
system

Keywords **snmp**
Prompts you in a line-by-line fashion to change SNMP configuration settings. Table B-17 describes the SNMP fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table B-17. SNMP Configuration Settings

Entry	Description
SNMPEnabled	Enables (True) or disables (False) SNMP on the switch. The default is True.
Contact	Specifies the name of the person to be contacted to respond to trap events. The default is undefined.
Location	Specifies the name of the switch location. The default is undefined.
Trap [1-5] Address	Specifies the workstation IP address to which SNMP traps are sent. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0. Addresses, other than 0.0.0.0, for all traps must be unique.
Trap [1-5] Port	Specifies the workstation port to which SNMP traps are sent. The default is 162.
Trap [1-5] Severity	Specifies the severity level to use when monitoring trap events. The default is Warning
Trap [1-5] Version	Specifies the SNMP version (1 or 2) to use in formatting traps. The default is 2.
Trap [1-5] Enabled	Specifies whether traps (event information) are enabled or disabled (default).
ReadCommunity	Read community password that authorizes an SNMP agent to read information from the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “public”.

Table B-17. SNMP Configuration Settings (Continued)

Entry	Description
WriteCommunity	Write community password that authorizes an SNMP agent to write information to the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “private”.
TrapCommunity	Trap community password that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “public”.
AuthFailureTrap	Enables (True) or disables (False) the generation of traps in response to trap authentication failures. The default is False.
ProxyEnabled	Enables (True) or disables (False) SNMP communication with other switches in the fabric. The default is True.

system
Prompts you in a line-by-line fashion to change system configuration settings. Table B-18 describes the system configuration fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Note: Changing the IP address will terminate all Ethernet management sessions.

Table B-18. System Configuration Settings

Entry	Description
Eth0NetworkDiscovery	Ethernet boot method: 1 - Static, 2 - Bootp, 3 - DHCP, 4 - RARP. The default is 1 - Static.
Eth0NetworkAddress	Ethernet Internet Protocol (IP) address. The default is 10.0.0.1.
Eth0NetworkMask	Ethernet subnet mask address.
Eth0GatewayAddress	Ethernet IP address gateway.
FCNetworkDiscovery	Fibre Channel boot method: 1 - Static, 3 - DHCP. The default is 1 - Static.
FCNetworkAddress	Fibre Channel Internet Protocol (IP) address for the Ethernet port. The default is 0.0.0.0.

Table B-18. System Configuration Settings (Continued)

Entry	Description
FCNetworkMask	Fibre Channel subnet mask address. The default is 255.0.0.0.
FCGatewayAddress	Fibre Channel IP address gateway. The default is 10.0.0.254.
AdminTimeout	Specifies the amount of time in minutes the switch waits before terminating an idle Admin session. Zero (0) disables the time out threshold. The default is 30, the maximum is 1440.
TempMonitoringWarning	Warning temperature threshold in °C above which a warning condition alarm is generated. The default is 65 °C.
TempMonitoringFailure	Failure temperature threshold in °C above which a failure condition alarm is generated. The default is 70 °C.
TempFailurePortShutdown	Enables (True) or disables (False) the switch's ability to place all ports down when the internal temperature exceeds the failure threshold. The default is False.
UserAuthentication	Enables (True) or disables (False) the enforcement of account names and passwords for SANbox Manager. The default is False.
LocalLogEnabled	Enables (True) or disables (False) the saving of log information on the switch. The default is True.
RemoteLogEnabled	Enables (True) or disables (False) the recording of the switch event log on a remote host that supports the syslog protocol. The default is False.
RemoteLogHostAddress	The IP address of the host that will receive the switch event log information if remote logging is enabled. The default is 10.0.0.254.

Examples

The following is an example of the Set Setup SNMP command:

```
SANbox2 #> admin start
SANbox2 (admin) #> set setup snmp
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
```

```
Trap Severity Options
---------------------
unknown, emergency, alert, critical, error, warning, notify, info, debug, mark

SNMPEnabled         (True / False)               [True             ]
Contact             (string, max=32 chars)       [<sysContact undefined]
Location            (string, max=32 chars)       [sysLocation undefined]
Trap1Address        (dot-notated IP Address)     [10.20.71.15      ]
Trap1Port           (decimal value)              [162              ]
Trap1Severity       (see allowed options above)  [warning          ]
Trap1Version        (1 / 2)                      [2                ]
Trap1Enabled        (True / False)               [False            ]
Trap2Address        (dot-notated IP Address)     [0.0.0.0          ]
Trap2Port           (decimal value)              [162              ]
Trap2Severity       (see allowed options above)  [warning          ]
Trap2Version        (1 / 2)                      [2                ]
Trap2Enabled        (True / False)               [False            ]
Trap3Address        (dot-notated IP Address)     [0.0.0.0          ]
Trap3Port           (decimal value)              [162              ]
Trap3Severity       (see allowed options above)  [warning          ]
Trap3Version        (1 / 2)                      [2                ]
Trap3Enabled        (True / False)               [False            ]
Trap4Address        (dot-notated IP Address)     [0.0.0.0          ]
Trap4Port           (decimal value)              [162              ]
Trap4Severity       (see allowed options above)  [warning          ]
Trap4Version        (1 / 2)                      [2                ]
Trap4Enabled        (True / False)               [False            ]
Trap5Address        (dot-notated IP Address)     [0.0.0.0          ]
Trap5Port           (decimal value)              [162              ]
Trap5Severity       (see allowed options above)  [warning          ]
Trap5Version        (1 / 2)                      [2                ]
Trap5Enabled        (True / False)               [False            ]
ReadCommunity       (string, max=32 chars)       [public           ]
WriteCommunity      (string, max=32 chars)       [private          ]
TrapCommunity       (string, max=32 chars)       [public           ]
AuthFailureTrap     (True / False)               [False            ]
ProxyEnabled        (True / False)               [True             ]
```

The following is an example of the Set Setup System command:

```
SANbox2 (admin) #> set setup system
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

Eth0NetworkDiscovery    (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp)  [Static       ]
Eth0NetworkAddress      (dot-notated IP Address)             [10.0.0.1     ]
Eth0NetworkMask         (dot-notated IP Address)             [255.255.255.0]
Eth0GatewayAddress      (dot-notated IP Address)             [10.0.0.254   ]
FCNetworkDiscovery      (1=Static, 3=Dhcp)                   [Static       ]
FCNetworkAddress        (dot-notated IP Address)             [0.0.0.0      ]
FCNetworkMask           (dot-notated IP Address)             [255.0.0.0    ]
FCGatewayAddress        (dot-notated IP Address)             [10.0.0.254   ]
AdminTimeout            (dec value 0-1440 minutes, 0=never)  [30           ]
TempMonitoringWarning   (dec value 0-100 degrees Celsius)    [65           ]
TempMonitoringFailure   (dec value 0-100 degrees Celsius)    [70           ]
TempFailurePortShutdown (True / False)                       [False        ]
UserAuthentication      (True / False)                       [False        ]
LocalLogEnabled         (True / False)                       [True         ]
RemoteLogEnabled        (True / False)                       [False        ]
RemoteLogHostAddress    (dot-notated IP Address)             [10.0.0.254   ]
```

Show Command

Displays fabric, switch, and port operational information.

Authority None

Syntax **show**
about
alarm
broadcast
chassis
config [option]
domains
donor
fabric
fdmi *[node_wwn]*
interface
log *[option]*
lsdb
mem [count]
ns *[option]*
pagebreak
perf *[option]*
port *[port_number]*
post log
setup [option]
steering *[domain_id]*
support
switch
topology
users
version

Keywords

about
Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the Version keyword.

alarm
Displays the last 200 alarm entries.

broadcast
Displays the broadcast tree information and all ports that are currently transmitting and receiving broadcast frames.

chassis
Displays chassis component status and temperature.

config [option]
Displays switch, port, and zoning configuration attributes. Refer to the ”Show Config Command” on page B-72.

domains
Displays list of each domain and its worldwide name in the fabric.

donor
Displays list of current donor configuration for all ports.

fabric
Displays list of each domain, symbolic name, worldwide name, node IP address, and port IP address.

fdmi ***[node_wwn]***
Displays information (worldwide name, manufacturer, model, and number of ports) for the device host bus adapter given by [node_wwn]. If you omit [node_wwn], the command displays host bus adapter information for all attached devices.

interface
Displays the status of the active network interfaces.

log ***[option]***
Displays log entries. Refer to the ”Show Log Command” on page B-75.

lsdb
Displays Link State database information.

mem [count]
Displays information about memory activity for the number of seconds given by [count]. If you omit [count], the value 1 is used. Displayed memory values are in 1K block units.

Note: This keyword will display memory activity updates until [count] is reached – it cannot be interrupted. Therefore, avoid using large values for [count].

ns ***[option]***
Displays name server information for the specified [option]. If you omit [option], name server information for the local domain ID is displayed. [option] can have the following values:

all
Displays name server information for all switches and ports.

[domain_id]
Displays name server information for the switch given by [domain_id]. [domain_id] is a switch domain ID.

[port_id]
Displays name server information for the port given by [port_id]. [port_id] is a port Fibre Channel address.

pagebreak
Displays the current pagebreak setting. The pagebreak setting limits the display of information to 20 lines (On) or allows the continuous display of information without a break (Off).

perf *[option]*
Displays performance information for all ports. Refer to the "Show Perf Command" on page B-77.

port *[port_number]*
Displays operational information for the port given by [port_number]. Ports are numbered beginning with 0. If [port number] is omitted, information is displayed for all ports. Table B-19 describes the port parameters.

Table B-19. Show Port Parameters

Entry	Description
AInit	Incremented each time the port begins AL initialization.
AInitError	Number of times the port entered initialization and the initialization failed.
Bad Frames	Number of frames that have framing errors.
ClassXFramesIn	Number of class *x* frames received by this port.
ClassXFramesOut	Number of class *x* frames sent by this port.
ClassXWordsIn	Number of class *x* words received by this port.
ClassXWordsOut	Number of class *x* words sent by this port.
ClassXToss	Number of times an SOFi3 or SOFn3 frame is tossed from TBUF.
DecodeError	Number of decode errors detected
EpConnects	Number of times an E_Port connected through ISL negotiation.
FBusy	Number of times the switch sent a F_BSY because Class 2 frame could not be delivered within ED_TOV time. Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_Port that is preventing delivery of this frame.
Flowerrors	Received a frame when there were no available credits.
FReject	Number of frames from devices that were rejected.
InvalidCRC	Invalid CRC detected.

Table B-19. Show Port Parameters (Continued)

Entry	Description
InvalidDestAddr	Invalid destination address detected.
LIP ALPD ALPS	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed.
LIPF7ALPS	This LIP is used to reinitialize the loop. An L_Port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.
LIPF8ALPS	This LIP denotes a loop failure detected by the L_Port identified by AL_PS.
LIPF7F7	A loop initialization primitive frame used to acquire a valid AL_PA.
LIPF8F7	A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver.
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or by loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established, a link failure is counted. A link reset is performed after a link failure.
Login	Number of device logins
Logout	Number of device logouts
LoopTimeouts	A two (2) second timeout as specified by FC-AL-2.
LossOfSync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
PrimSeqErrors	Primitive sequence errors detected.
RxLinkResets	Number of link reset primitives received from an attached device.
RxOfflineSeq	Number of offline sequences received. An OLS is issued for link initialization, a Receive & Recognize Not_Operational (NOS) state, or to enter the offline state.
TotalErrors	Total number of errors detected.
TotalLIPsRecvd	Number of loop initialization primitive frames received by this port.

Table B-19. Show Port Parameters (Continued)

Entry	Description
TotalLIPsXmitd	Number of loop initialization primitive frames transmitted by this port.
TotalLinkResets	Total number of link reset primitives.
TotalOfflineSeq	Total number of Offline Sequences issued and received by this port.
TotalRxFrames	Total number of frames received by this port.
TotalRxWords	Total number of words received by this port.
TotalTxFrames	Total number of frames issued by this port.
TotalTxWords	Total number of words issued by this port.
TxLinkResets	Number of Link Resets issued by this port.
TxOfflineSeq	Total number of Offline Sequences issued by this port.
TxWaits	Time waiting to transmit when blocked with no credit. Measured in FC Word times.

post log
Displays the Power On Self Test (POST) log which contains results from the POST.

setup [option]
Displays setup attributes for the system, SNMP, and the switch manufacturer. Refer to the ”Show Setup Command” on page B-79.

steering *[domain_id]*
Displays the routes that data takes to the switch given by [domain_id]. If you omit [domain_id], the system displays routes for all switches in the fabric.

support
Executes a series of commands that display a complete description of the switch, its configuration, and operation. The display can be captured from the screen and used for diagnosing problems. This keyword is intended for use at the request of your authorized maintenance provider. The commands that are executed include the following:

- Alias List
- Config List
- Date
- Group List

- History
- Ps
- Security (List, Limits, History)
- Securityset (Active, List)
- Show (About, Alarm, Backtrace, Chassis, Config Port, Config Security, Config Switch, Config Threshold, Dev, Dev Settings, Domains, Donor, Fabric, Log, Log Settings, Lsdb, Mem, Ns, Perf, Port, Setup Mfg, Setup Snmp, Setup System, Steering, Switch, Topology, Users)
- Uptime
- User Accounts
- Whoami
- Zoneset (Active, List)
- Zoning (History, Limits, List)

switch
Displays switch operational information.

topology
Displays all connected devices.

users
Displays a list of logged-in users. This is equivalent to the User List command.

version
Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the About keyword.

Examples

The following is an example of the Show Chassis command:

```
SANbox2 #> show chassis
    Chassis Information
  ------------------
  BoardTemp (1) - Degrees Celsius   32
  BoardTemp (2) - Degrees Celsius   36
  FanStatus (1)                     Good
  FanStatus (2)                     Good
  PowerSupplyStatus (1)             Good
  PowerSupplyStatus (2)             Good
  HeartBeatCode                     1
  HeartBeatStatus                   Normal
```

The following is an example of the Show Domains command:

```
SANbox2 #> show domains
  Principal switch is (remote): 10:00:00:60:69:50:0b:6c
  Upstream Principal ISL is   : 1
  Domain ID List:
        Domain 97  (0x61)  WWN = 10:00:00:c0:dd:00:71:ed
        Domain 98  (0x62)  WWN = 10:00:00:60:df:22:2e:0c
        Domain 99  (0x63)  WWN = 10:00:00:c0:dd:00:72:45
        Domain 100 (0x64)  WWN = 10:00:00:c0:dd:00:ba:68
        Domain 101 (0x65)  WWN = 10:00:00:60:df:22:2e:06
        Domain 102 (0x66)  WWN = 10:00:00:c0:dd:00:90:ef
        Domain 103 (0x67)  WWN = 10:00:00:60:69:50:0b:6c
        Domain 104 (0x68)  WWN = 10:00:00:c0:dd:00:b8:b7
```

The following is an example of the Show Fabric command:

```
SANbox2 #> show fabric

 Domain     WWN                     Enet IP Addr    FC IP Addr      SymbolicName
 ------     ---                     ------------    ----------      ------------
 16 (0x10)  10:00:00:c0:dd:00:77:81 10.20.68.11     0.0.0.0         gui sb1 .11
 17 (0x11)  10:00:00:c0:dd:00:6a:2d 10.20.68.12     0.0.0.0         sw12
 18 (0x12)  10:00:00:c0:dd:00:c3:04 10.20.68.160    0.0.0.0         sw .160
 19 (0x13)  10:00:00:c0:dd:00:bc:56 10.20.68.108    0.0.0.0         Sb2 .108
```

The following is an example of the Show FDMI command:

```
SANbox2 #> show fdmi

HBA ID                  Manufacturer Model     Ports
--------                ---------------        ------- -----
20:00:00:00:c9:25:9b:96 Emulex Network Systems LP9000  2
20:00:00:00:ca:25:9b:96 QLogic Corporation     QL2330  2
```

The following is an example of the Show FDMI WWN command:

```
SANbox2 #> show fdmi 21:00:00:e0:8b:09:3b:17
  FDMI Information
  -----------------
  Manufacturer                    QLogic Corporation
  SerialNumber                    95923
  Model                           QCP2340
  ModelDescription
  NodeWWN                         20:00:00:e0:8b:09:3b:17
  HardwareVersion                 A
  DriverVersion                   4.12 Beta 21
  OptionRomVersion
  FirmwareVersion                 3.2.15
  OSSystemName                    SunOS 5.8
  MaximumCTPayload
  NumberOfPorts                   1

  Port  21:00:00:e0:8b:09:3b:17

  SupportedFC4Types               FCP
  SupportedSpeed                  2Gb/s
  CurrentSpeed                    2Gb/s
  MaximumFrameSize                2048
  OSDeviceName                    qla2300(0)
```

The following is an example of the Show NS (local domain) command:

```
SANbox2 #> show ns
  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   19 (0x13) 1301e1 NL   3   21:00:00:20:37:73:13:69 20:00:00:20:37:73:13:69
  2   19 (0x13) 1301e2 NL   3   21:00:00:20:37:73:12:9b 20:00:00:20:37:73:12:9b
  3   19 (0x13) 1301e4 NL   3   21:00:00:20:37:73:05:26 20:00:00:20:37:73:05:26
  4   19 (0x13) 130d00 N    3   21:01:00:e0:8b:27:a7:bc 20:01:00:e0:8b:27:a7:bc
```

The following is an example of the Show NS [domain_ID] command:

```
SANbox2 #> show ns 18
    Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   18 (0x12) 120700 N    3   21:00:00:e0:8b:07:a7:bc 20:00:00:e0:8b:07:a7:bc
```

The following is an example of the Show NS [port_ID] command:

```
SANbox2 #> show ns 1301e1
  Port ID: 1301e1
  --------
  PortType          NL
  PortWWN           21:00:00:20:37:73:13:69
  SymbolicPortName
  NodeWWN           20:00:00:20:37:73:13:69
  SymbolicNodeName
  NodeIPAddress     0.0.0.0
  ClassOfService    3
  PortIPAddress     0.0.0.0
  FabricPortName    20:01:00:c0:dd:00:bc:56
  FC4Type           FCP
  FC4Desc           (NULL)
```

The following is an example of the Show Interface command:

```
SANbox2 #> show interface
eth0      Link encap:Ethernet  HWaddr 00:C0:DD:00:BD:ED
          inet addr:10.20.68.107  Bcast:10.20.68.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4712 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3000 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:415313 (405.5 Kb)  TX bytes:716751 (699.9 Kb)
          Interrupt:11 Base address:0xfcc0
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:304 errors:0 dropped:0 overruns:0 frame:0
          TX packets:304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20116 (19.6 Kb)  TX bytes:20116 (19.6 Kb)
```

The following is an example of the Show Port command:

```
SANbox2 #> show port 1
    Port Number: 1
  ------------
  AdminState       Online             PortID           150100
  AsicNumber       0                  PortWWN          20:01:00:c0:dd:00:bc:b8
  AsicPort         1                  RunningType      Unknown
  ConfigType       G                  SFPPartNumber    Unknown
  DiagStatus       Passed             SFPRevision      0
  EpConnState      None               SFPType          NotInstalled
  EpIsoReason      NotApplicable      SFPVendor        Unknown
  LinkSpeed        2Gb/s              SFPVendorID      00000000
  LinkState        Inactive           SymbolicName     Port1
  LoginStatus      NotLoggedIn        SyncStatus       SyncLost
  MaxCredit        12                 XmitterEnabled   True
  OperationalState Offline

  ALInit          0                    LIP_F8_AL_PS    0
  ALInitError     0                    LIP_F8_F7       0
  BadFrames       0                    LinkFailures    26
  Class2FramesIn  0                    Login           25
  Class2FramesOut 0                    Logout          24
  Class2WordsIn   0                    LoopTimeouts    0
  Class2WordsOut  0                    LossOfSync      1
  Class3FramesIn  0                    PrimSeqErrors   0
  Class3FramesOut 0                    RxLinkResets    23
  Class3Toss      0                    RxOfflineSeq    45
  Class3WordsIn   0                    TotalErrors     26
  Class3WordsOut  0                    TotalLIPsRecvd  0
  DecodeErrors    0                    TotalLIPsXmitd  0
  EpConnects      25                   TotalLinkResets 77
  FBusy           0                    TotalOfflineSeq 59
  FlowErrors      0                    TotalRxFrames   0
  FReject         0                    TotalRxWords    0
  InvalidCRC      0                    TotalTxFrames   0
  InvalidDestAddr 0                    TotalTxWords    0
  LIP_AL_PD_AL_PS 0                    TxLinkResets    54
  LIP_F7_AL_PS    0                    TxOfflineSeq    14
  LIP_F7_F7       0                    TxWaits         222649090
```

The following is an example of the Show Switch command:

```
SANbox2 #> show switch
Switch Information
------------------
SymbolicName                     sw .108
SwitchWWN                        100000c0dd00bc56
SwitchType                       SANbox2-16
PROMVersion                      V2.0.0.0-0 (day month date time year)
CreditPool                       0
DomainID                         19 (0x13)
FirstPortAddress                 130000
FlashSize - MBytes               128
LogLevel                         Critical
MaxPorts                         16
NumberOfResets                   224
ReasonForLastReset               PowerUp
SWImageVersion (1) - build date  V2.0.0.0-17 (day month date time year)
SWImageVersion (2) - build date  V2.0.0.0-17 (day month date time year)
ActiveImageVersion - build date  V2.0.0.0-2 (day month date time year)
PendingImageVersion - build date V2.0.0.0-17 (day month date time year)
ActiveConfiguration              default
AdminState                       Online
AdminModeActive                  False
BeaconOnStatus                   False
OperationalState                 Online
PrincipalSwitchRole              False
BoardTemp (1) - Degrees Celsius  32
BoardTemp (2) - Degrees Celsius  36
SwitchDiagnosticsStatus          Passed
SwitchTemperatureStatus          Normal
```

The following is an example of the Show Topology command:

```
SANbox2 #> show topology
Unique ID Key
-------------
A = ALPA,  D = Domain ID,  P = Port ID
Port   Local Local                    Remote  Remote                    Unique
Number Type  PortWWN                  Type    NodeWWN                   ID
------ ----- -------                  ------  -------                   ------
5      F     20:05:00:c0:dd:00:bd:ec   N      20:00:00:00:c9:22:1e:93   010500 P
10     E     20:0a:00:c0:dd:00:bd:ec   E      10:00:00:c0:dd:00:80:21   4(0x4) D
```

The following is an example of the Show Topology command for port 1:

```
SANbox2  #> show topology 1
  Local Link Information
  ----------------------
  PortNumber 1
  PortID     650100
  PortWWN    20:01:00:c0:dd:00:91:11
  PortType   F

Remote Link Information
-----------------------
Device 0
NodeWWN 50:80:02:00:00:06:d5:38
PortType NL
Description (NULL)
IPAddress 0.0.0.0

Device 1
NodeWWN 20:00:00:20:37:2b:08:c9
PortType NL
Description (NULL)
IPAddress 0.0.0.0

Device 2
Description (NULL)
IPAddress 0.0.0.0

Device 3
NodeWWN 20:00:00:20:37:2b:05:c9
PortType NL
Description (NULL)
IPAddress 0.0.0.0
```

The following is an example of the Show Version command:

```
SANbox2 #> show version
       ************************************************
       *                                              *
       *       Command Line Interface SHell  (CLISH)  *
       *                                              *
       ************************************************

       SystemDescription  QLogic SANbox2 FC Switch
       Eth0NetworkAddress 10.20.11.192 (use 'set setup system' to update)
       FCNetworkAddress   0.0.0.0 (use 'set setup system' to update)
       MACAddress         00:c0:dd:00:71:ee
       WorldWideName      10:00:00:c0:dd:00:71:ed
       SymbolicName       SB211.192
       ActiveSWVersion    V2.0.0.0-26
       ActiveTimestamp    day month date time year
       DiagnosticsStatus  Passed
       SecurityEnabled    True
```

Show Config Command

Displays switch, port, alarm threshold, security, and zoning for the current configuration.

Authority None

Syntax **show config**
port *[port_number]*
security
switch
threshold
zoning

Keywords **port *[port_number]***
Displays configuration parameters for the port number given by [port_number]. Ports are numbered beginning with 0. If [port_number] is omitted, all ports are specified.

security
Displays the security database Autosave parameter value.

switch
Displays configuration parameters for the switch.

threshold
Displays alarm threshold parameters for the switch.

zoning
Displays zoning configuration parameters for the switch.

Examples The following is an example of the Show Config Port command:

```
SANbox2 #> show config port 3
    Port Number: 3
  ------------
  AdminState         Offline
  LinkSpeed          Auto
  PortType           GL
  SymbolicName       Port3
  ALFairness         False
  DeviceScanEnabled  True
  ForceOfflineRSCN   False
  ARB_FF             False
  InteropCredit      0
  ExtCredit          0
  FANEnabled         True
  LCFEnabled         False
  MFSEnabled         True
  MSEnabled          True
```

```
NoClose            False
IOStreamGuard      Disabled
VIEnabled          False
```

The following is an example of the Show Config Switch command:

```
SANbox2 #> show config switch

  Switch Configuration Information
  --------------------------------
  AdminState            Online
  BroadcastEnabled      False
  InbandEnabled         True
  FDMIEnabled           False
  FDMIEntries           10
  DomainID              19 (0x13)
  DomainIDLock          True
  SymbolicName          sw108
  R_A_TOV               10000
  E_D_TOV               2000
  PrincipalPriority     254
  ConfigDescription     QLogic SANbox2 FC Switch
  ConfigLastSavedBy     admin@OB-session5
  ConfigLastSavedOn     day month date time year
  FC-SW-2 Compliant     True
  Legacy Address Format False[1]
```

The following is an example of the Show Config Threshold command:

```
SANbox2 #> show config threshold
Configuration Name: default
------------

  Threshold Configuration Information
  -----------------------------------
  ThresholdMonitoringEnabled    False
  CRCErrorsMonitoringEnabled    True
  RisingTrigger                 25
  FallingTrigger                1
  SampleWindow                  10
  DecodeErrorsMonitoringEnabled True
  RisingTrigger                 25
  FallingTrigger                0
```

[1] Appears only if FC-SW-2 Compliant is False.

```
  SampleWindow                10
  ISLMonitoringEnabled        True
  RisingTrigger               2
  FallingTrigger              0
  SampleWindow                10
  LoginMonitoringEnabled      True
  RisingTrigger               5
  FallingTrigger              1
  SampleWindow                10
  LogoutMonitoringEnabled     True
  RisingTrigger               5
  FallingTrigger              1
  SampleWindow                10
  LOSMonitoringEnabled        True
  RisingTrigger               100
  FallingTrigger              5
  SampleWindow                10
```

The following is an example of the Show Config Zoning command:

```
SANbox2 #> show config zoning

 Configuration Name: default
  -------------------

  Zoning Configuration Information
  --------------------------------
  FC-SW-2 AutoSave      True
  Default Visibility    All
```

Show Log Command

Displays the contents of the log or the parameters used to create entries in the log. The log contains a maximum of 200 entries. When the log reaches its entry capacity, subsequent entries overwrite the existing entries, beginning with the oldest.

Authority None

Syntax **show log**
component
level
options
port
settings

Keywords **component**
Displays the components currently being monitored for events.

level
Displays the event severity level needed to create an entry in the log. If the severity level occurs on a port or on a component which is not defined, no entry is made in the log.

options
Displays the options used to set the component and log level attributes.

port
Displays the ports being monitored for events. If an event occurs which is of the defined level and on a defined component, but not on a defined port, no entry is made in the log.

settings
Displays the current settings for component, level and port. This command is equivalent to executing the following commands separately: Show Log Component, Show Log Level, and Show Log Port.

Examples The following is an example of the Show Log Component command:

```
SANbox2 #> show log component

  Current setting(s) for log component: NameServer
```

The following is an example of the Show Log Level command:

```
SANbox2 #> show log level
  Current settings for log
  ------------------------
  level      Critical
```

The following is an example of the Show Log Options command:

```
SANbox2 #> show log options
  Allowed options for log
  ----------------------
  component  All, None, NameServer, MgmtServer, Zoning, Switch, Chassis, Blade,
             Port, Eport, Snmp, Other,CimServer
  level      Critical,Warn,Info,None
```

The following is an example of the Show Log command:

```
[327][day month date time year][I][Eport Port:0/8][Eport State=
E_A0_GET_DOMAIN_ID]
[328][day month date time year][I][Eport Port: 0/8][FSPF PortUp state=0]
[329][day month date time year][I][Eport Port: 0/8][Sending init hello]
[330][day month date time year][I][Eport Port: 0/8][Processing EFP, oxid= 0x8]
[331][day month date time year][I][Eport Port: 0/8][Eport State = E_A2_IDLE]
[332][day month date time year][I][Eport Port: 0/8][EFP,WWN= 0x100000c0dd00b845,
len= 0x30]
[333][day month date time year][I][Eport Port: 0/8][Sending LSU oxid=0xc:type=1]
[334][day month date time year][I][Eport Port: 0/8][Send Zone Merge Request]
[335][day month date time year][I][Eport Port: 0/8][LSDB Xchg timer set]
[336][day month date time year][I][Eport Port: 0/8][Setting attribute
Oper.UserPort.0.8.EpConnState Connected]
```

Show Perf Command

Displays port performance in frames/second and bytes/second. If you omit the keyword, the command displays data transmitted (out), data received (in), and total data transmitted and received in frames/second and bytes per second.

Authority None

Syntax

show perf
- byte
- inbyte
- outbyte
- frame
- inframe
- outframe
- errors

Keywords

byte
Displays continuous performance data in total bytes/second transmitted and received for all ports. Type “q” and press the Enter key to stop the display.

inbyte
Displays continuous performance data in bytes/second received for all ports. Type “q” and press the Enter key to stop the display.

outbyte
Displays continuous performance data in bytes/second transmitted for all ports. Type “q” and press the Enter key to stop the display.

frame
Displays continuous performance data in total frames/second transmitted and received for all ports. Type “q” and press the Enter key to stop the display.

inframe
Displays continuous performance data in frames/second received for all ports. Type “q” and press the Enter key to stop the display.

outframe
Displays continuous performance data in frames/second transmitted for all ports. Type “q” and press the Enter key to stop the display.

errors
Displays continuous error counts for all ports. Type “q” and press the Enter key to stop the display.

Examples The following is an example of the Show Perf command:

```
SANbox2 #> show perf
Port   Bytes/s    Bytes/s    Bytes/s    Frames/s   Frames/s   Frames/s
  Number   (in)       (out)    (total)      (in)       (out)    (total)
  ------ -------    -------    -------    --------   --------   --------
  0      0          0          0          0          0          0
  1      0          0          0          0          0          0
  2      0          0          0          0          0          0
  3      0          0          0          0          0          0
  4      0          0          0          0          0          0
  5      0          0          0          0          0          0
  6      0          0          0          0          0          0
  7      0          0          0          0          0          0
  8      7K         136M       136M       245        68K        68K
  9      58K        0          58K        1K         0          1K
  10     0          0          0          0          0          0
  11     0          0          0          0          0          0
  12     0          0          0          0          0          0
  13     0          0          0          0          0          0
  14     0          7K         7K         0          245        245
  15     136M       58K        136M       68K        1K         70K
```

The following is an example of the Show Perf Byte command:

```
SANbox2 #> show perf byte
Displaying bytes/sec (total)...  (Press 'q' and the ENTER key to stop display)

  0    1    2    3    4    5    6    7    8    9    10   11   12   13   14   15
  ------------------------------------------------------------------------------
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    8K   136M
  0    0    0    0    0    0    0    0    135M 58K  0    0    0    0    7K   135M
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    7K   136M
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    8K   136M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    7K   136M
q
```

Show Setup Command

Displays the current SNMP and system settings.

Authority None

Syntax **show setup**
mfg
snmp
system

Keywords **mfg**
Displays manufacturing information about the switch.

snmp
Displays the current SNMP settings.

system
Displays the current system settings.

Examples The following is an example of the Show Setup Mfg command:

```
SANbox2 #> show setup mfg
    Manufacturing Information
  ------------------------
  BrandName               QLogic
  BuildDate               Unknown
  ChassisPartNumber       Unknown
  ChassisSerialNumber     0
  CPUBoardSerialNumber    000603949
  MACAddress              00:c0:dd:00:90:aa
  PlanarPartNumber        Unknown
  SwitchSymbolicName      SANbox2
  SwitchWWN               10:00:00:c0:dd:00:90:ab
  SystemDescription       QLogic SANbox2 FC Switch
  SystemObjectID          1.3.6.1.4.1.1663.1.1.1.1.11
```

The following is an example of the Show Setup Snmp command:

```
SANbox2 #> show setup snmp
  SNMP Information
  ----------------
  SNMPEnabled           True
  Contact               <sysContact undefined>
  Location              N_107 System Test Lab
  Description           QLogic SANbox2 FC Switch
  Trap1Address          10.0.0.254
  Trap1Port             162
  Trap1Severity         warning
  Trap1Version          2
  Trap1Enabled          False
  Trap2Address          0.0.0.0
  Trap2Port             162
  Trap2Severity         warning
  Trap2Version          2
  Trap2Enabled          False
  Trap3Address          0.0.0.0
  Trap3Port             162
  Trap3Severity         warning
  Trap3Version          2
  Trap3Enabled          False
  Trap4Address          0.0.0.0
  Trap4Port             162
  Trap4Severity         warning
  Trap4Version          2
  Trap4Enabled          False
  Trap5Address          0.0.0.0
  Trap5Port             162
  Trap5Severity         warning
  Trap5Version          2
  Trap5Enabled          False
  ObjectID              1.3.6.1.4.1.1663.1.1.1.1.11
  AuthFailureTrap       True
  ProxyEnabled          True
```

The following is an example of the Show Setup System command:

```
SANbox2 #> show setup system
  System Information
  ------------------
  Eth0NetworkDiscovery     Static
  Eth0NetworkAddress       10.20.11.32
  Eth0NetworkMask          255.255.252.0
  Eth0GatewayAddress       10.20.8.254
  FCNetworkDiscovery       Static
  FCNetworkAddress         0.0.0.0
  FCNetworkMask            255.0.0.0
  FCGatewayAddress         10.0.0.254
  AdminTimeout             30
  TempMonitoringWarning    65
  TempMonitoringFailure    70
  TempFailurePortShutdown  False
  UserAuthentication       False
  LocalLogEnabled          True
  RemoteLogEnabled         False
  RemoteLogHostAddress     10.0.0.254
```

Shutdown Command

Terminates all data transfers on the switch at convenient points and closes the Telnet session. Always power cycle the switch after entering this command.

Authority Admin session

Syntax **shutdown**

Notes Always use this command to perform an orderly shut down before removing power from the switch.

When the shutdown is complete, the Heartbeat LED is extinguished.

Test Command

Tests ports using internal (SerDes level), external (SFP), and online loopback tests. Internal and external tests require that the port be placed in diagnostic mode. Refer to the "Set Command" on page B-37 for information about changing the port administrative state. While the test is running, the remaining ports on the switch remain fully operational.

Authority Admin session

Syntax

test
port [port_number] [test_type]
cancel
status

Keywords

port [port_number] *[test_type]*
Tests the port given by [port_number] using the test given by [test_type]. If you omit [test_type], Internal is used. [test_type] can have the following values:

internal
Tests the SerDes. This is the default. The port must be in diagnostics mode to perform this test.

external
Tests both the SerDes and SFP. The port must be in diagnostics mode to perform this test, and a loopback plug must be installed in the SFP.

online
Tests one online port.

cancel
Cancels the online test in progress.

status
Displays the status of a test in progress, or if there is no test in progress, the status of the test that was executed last.

Examples To run an internal (SerDes) or external (SFP) port test, do the following:

1. To start an admin session, enter the following command and press the Enter key.

```
admin start
```

2. Place the port in Diagnostics mode, enter the following command (*x* = port number) and press the Enter key.

```
set port x state diagnostics
```

3. Choose the type of port loopback test to run:
   - To run an internal loopback test, enter the following:

     ```
     test port x internal
     ```

   - To run an external loopback test, enter the following command. A loopback plug must be installed for this test to pass.

     ```
     test port x external
     ```

4. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload.
5. After the test type has been chosen and the command executed, a message on the screen will appear detailing the test results.
6. After the test is run, put the port back into online state by entering the following command (*x* = port number) and pressing the Enter key.

   ```
   set port x state online
   ```

7. To verify port is back online, enter the following command and press the Enter key. The contents of the AdminState field should display be “Online”.

   ```
   show port x
   ```

The online loopback (node-to-node) test requires that port be online and connected to a remote device. To run the online loopback test, do the following:

1. To start an admin session, enter the following command and press the Enter key.

   ```
   admin start
   ```

2. To run the online loopback test, enter the following command and press the Enter key.

   ```
   test port x online
   ```

3. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload. Before running the test, make sure that the device attached to the port can handle the test parameters.

```
SANbox2 (admin) #> test port x online

A list of attributes with formatting and current values will
follow. Enter a new value or simply press the ENTER key to
accept the default value. If you wish to terminate this
process before reaching the end of the list press 'q' or 'Q'
and the ENTER key to do so.

  TestLength    (decimal value, 1-4294967295)   [100    ]
  FrameSize     (decimal value, 36-2148)        [256    ]
  DataPattern   (32-bit hex value or 'Default') [Default]
  StopOnError   (True/False)                    [False  ]
  Do you want to start the test? (y/n) [n]
```

4. After all parameter values are defined, press the Y key to start the test.

Uptime Command

Displays the elapsed up time since the switch was last reset and reset method. A hot reset or non-disruptive firmware activation does not reset the elapsed up time reported by this command.

Authority None

Syntax **uptime**

Examples The following is an example of the Uptime command:

```
SANbox2 #> uptime

  Elapsed up time  : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)
  Reason last reset: NormalReset
```

User Command

Administers and displays user accounts.

Authority Admin account name and an Admin session. The Accounts and List keywords are available to all account names without an Admin session.

Syntax

user
accounts
add
delete [account_name]
edit
list

Keywords

accounts
Displays all user accounts that exist on the switch. This keyword is available to all account names without an Admin session.

add
Add a user account to the switch. You will be prompted for an account name, a password, authority, and an expiration date.

- A switch can have a maximum of 15 user accounts.
- Account names are limited to 15 characters; passwords must be 4–20 characters.
- Admin authority grants permission to use the Admin command to open an admin session, from which all commands can be entered. Without Admin authority, you are limited to view-only commands.
- The expiration date is expressed in the number of days until the account expires (2000 maximum). The switch will issue an expiration alarm every day for seven days prior to expiration. 0 (zero) specifies that the account has no expiration date.

delete [account_name]
Deletes the account name given by [account_name] from the switch.

edit
Initiates an edit session that prompts you for the account name for which to change the expiration date and authority.

list
Displays the list of users currently logged in and their session numbers. Provides the same function as the Show Users command. This keyword is available to all account names without an Admin session.

Notes User accounts are enforced only if the UserAuthentication parameter is set to True. The UserAuthentication default value is False. Refer to System keyword of the ”Set Setup Command” on page B-54 for information about setting the UserAuthentication parameter.

Examples

The following is an example of the User Accounts command:

```
SANbox2 (admin) #> user accounts

    Current list of user accounts
  ----------------------------
  images       (admin authority = False, never expires)
  admin        (admin authority = True , never expires)
  chuckca      (admin authority = False, never expires)
  gregj        (admin authority = True , never expires)
  fred         (admin authority = True , never expires)
```

The following is an example of the User Add command:

```
SANbox2 (admin) #> user add
    Press 'q' and the ENTER key to abort this command.
account name (1-15 chars)      : user1
account password (4-20 chars)  :

please confirm account password:

set account expiration in days (0-2000, 0=never): [0] 100

should this account have admin authority? (y/n): [n] y

OK to add user account 'user1' with admin authority
and to expire in 100 days?

Please confirm (y/n): [n] y
```

The following is an example of the User Edit command:

```
SB211.192 (admin) #> user edit

      Press 'q' and the ENTER key to abort this command.

  account name (1-15 chars)      : user1
  set account expiration in days (0-2000, 0=never): [0]
  should this account have admin authority? (y/n): [n]

  OK to modify user account 'davem' with no admin authority
  and to expire in 0 days?

  Please confirm (y/n): [n]
```

The following is an example of the User Delete command:

```
SANbox2 (admin) #> user del user3

  The user account will be deleted.  Please confirm (y/n): [n] y
```

The following is an example of the User List command:

```
SANbox2 (admin) #> user list

    User                          Ethernet Addr-Port    Logged in Since
    ----                          ------------------    ---------------
  admin@OB-session1             10.20.68.108-1031     day month date time year
  admin@OB-session2             10.20.68.108-1034     day month date time year
  snmp@OB-session3              Unknown               day month date time year
  snmp@IB-session4              Unknown               day month date time year
  admin@OB-session5             Unknown               day month date time year
```

Whoami Command

Displays the account name, session number, and switch domain ID for the Telnet session.

Authority None

Syntax **whoami**

Examples The following is an example of the Whoami command:

```
SANbox2 #> whoami

User name       : admin@session2
Switch name     : SANbox2
Switch domain ID: 21 (0x15)
```

Zone Command

Manages zones and zone membership on a switch. The Zone command defines members (ports/devices) for a single switch. Zones are members of zone sets.

Authority Admin session and a Zoning Edit session. Refer to the "Zoning Command" on page B-97 for information about starting a Zoning Edit session. The List, Members, and Zonesets keywords are available without an Admin session.

Syntax

zone
add [zone] [member_list]
copy [zone_source] [zone_destination]
create [zone]
delete [zone]
list
members [zone]
remove [zone] [member_list]
rename [zone_old [zone_new]
type [zone] *[zone_type]*
zonesets [zone]

Keywords

add [zone] [member_list]
Specifies one or more ports/devices given by [members] to add to the zone named [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. A zone can have a maximum of 2000 members. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs and port numbers are in decimal. Ports are numbered beginning with 0.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

The application verifies that the [members] format is correct, but does not validate that such a port exists.

copy [zone_source] [zone_destination]
Creates a new zone named [zone_destination] and copies the membership into it from the zone given by [zone_source].

create [zone]
Creates a zone with the name given by [zone]. An zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 1000 zones.

delete [zone]
Deletes the specified zone given by [zone] from the zoning database. If the zone is a member of the active zone set, the zone will not be removed from the active zone set until the active zone set is deactivated.

list
Displays a list of all zones and the zone sets of which they are members. This keyword does not require an Admin session.

members [zone]
Displays all members of the zone given by [zone]. This keyword does not require an Admin session.

remove [zone] [member_list]
Removes the ports/devices given by [member_list] from the zone given by [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs and port numbers are in decimal. Ports are numbered beginning with 0.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

rename [zone_old] [zone_new]
Renames the zone given by [zone_old] to the zone given by [zone_new].

type [zone] ***[zone_type]***
Specifies the zone type given by [zone_type] to be assigned to the zone name given by [zone]. If you omit the [zone_type], the system displays the zone type for the zone given by [zone]. [zone_type] can be one of the following:

soft
Name server zone

hardACL
Access control list hard zone. This keyword is case sensitive.

hardVPF
Virtual private fabric hard zone. This keyword is case sensitive.

zonesets [zone]
Displays all zone sets of which the zone given by [zone] is a member. This keyword does not require an Admin session.

Examples

The following is an example of the Zone List command:

```
SANbox2 #> zone list

  Zone        ZoneSet
  -------------------
  wwn_b0241f
              zone_set_1

  wwn_23bd31
              zone_set_1

  wwn_221416
              zone_set_1

  wwn_2215c3
              zone_set_1

  wwn_0160ed
              zone_set_1

  wwn_c001b0
              zone_set_1

  wwn_401248
              zone_set_1

  wwn_02402f
              zone_set_1

  wwn_22412f
              zone_set_1
```

The following is an example of the Zone Members command:

```
SANbox2 #> zone members wwn_b0241f

  Current List of Members for Zone: wwn_b0241f
  --------------------------------
  50:06:04:82:bf:d2:18:c2
  50:06:04:82:bf:d2:18:d2
  21:00:00:e0:8b:02:41:2f
```

The following is an example of the Zone Zonesets command:

```
SANbox2 #> zone zonesets zone1

  Current List of ZoneSets for Zone: wwn_b0241f
  ---------------------------------
  zone_set_1
```

Zoneset Command

Manages zone sets and zone set membership across the fabric.

Authority Admin session and a Zoning Edit session. Refer to the "Zoning Command" on page B-97 for information about starting a Zoning Edit session. The Active, List, and Zones keywords are available without an Admin session. You must close the Zoning Edit session before using the Activate and Deactivate keywords.

Syntax

zoneset
activate [zone_set]
active
add [zone_set] [zone_list]
copy [zone_set_source] [zone_set_destination]
create [zone_set]
deactivate
delete [zone_set]
list
remove [zone_set] [zone_list]
rename [zone_set_old] [zone_set_new]
zones [zone_set]

Keywords

activate [zone_set]
Activates the zone set given by [zone_set]. This keyword deactivates the active zone set. Close the Zoning Edit session before using this keyword.

active
Displays the name of the active zone set. This keyword does not require Admin session.

add [zone_set] [zone_list]
Adds a list of zones and aliases given by [zone_list] to the zone set given by [zone_set]. Use a <space> to delimit zone and alias names in [zone_list]. This keyword requires a Zoning Edit session.

copy [zone_set_source] [zone_set_destination]
Creates a new zone set named [zone_set_destination] and copies into it the membership from the zone set given by [zone_set_source].

create [zone_set]
Creates the zone set with the name given by [zone_set]. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 256 zone sets.

deactivate
Deactivates the active zone set. Close the Zoning Edit session before using this keyword.

delete [zone_set]
Deletes the zone set given by [zone_set]. If the specified zone set is active, the command is suspended until the zone set is deactivated.

list
Displays a list of all zone sets. This keyword does not require an Admin session.

remove [zone_set] [zone_list]
Removes a list of zones given by [zone_list] from the zone set given by [zone_set]. Use a <space> to delimit zone names in [zone_list]. If [zone_set] is the active zone set, the zone will not be removed until the zone set has been deactivated. This keyword requires a Zoning Edit session.

rename [zone_set_old] [zone_set_new]
Renames the zone set given by [zone_set_old] to the name given by [zone_set_new]. You can rename the active zone set. This keyword requires a Zoning Edit session.

zones [zone_set]
Displays all zones that are members of the zone set given by [zone_set]. This keyword does not require an Admin session.

Notes

- A zone set must be active for its definitions to be applied to the fabric.
- Only one zone set can be active at one time.
- A zone can be a member of more than one zone set.

Examples

The following is an example of the Zoneset Active command:

```
SANbox2 #> zoneset active

  ActiveZoneSet    Bets
  LastActivatedBy  admin@OB-session6
  LastActivatedOn  day month date time year
```

The following is an example of the Zoneset List command:

```
SANbox2 #> zoneset list

  Current List of ZoneSets
  ------------------------
  alpha
  beta
```

The following is an example of the Zoneset Zones command:

```
SANbox2 #> zoneset zones ssss

  Current List of Zones for ZoneSet: ssss
  ---------------------------------
  zone1
  zone2
  zone3
```

Zoning Command

Opens a Zoning Edit session in which to create and manage zone sets and zones. Refer to the ”Zone Command” on page B-91 and the ”Zoneset Command” on page B-95.

Authority Admin session. The List keyword is available without Admin session nor a Zoning Edit session.

Syntax

zoning
- active
- cancel
- clear
- edit
- history
- limits
- list
- restore
- save

Keywords

active
Displays membership information for the active zone set including member zones and zone members.

cancel
Closes the current Zoning Edit session. Any unsaved changes are lost.

clear

Clears all inactive zone sets from the volatile edit copy of the zoning database. This keyword does not affect the non-volatile zoning database. However, if you enter the Zoning Clear command followed by the Zoning Save command, the non-volatile zoning database will be cleared from the switch.

Note: The preferred method for clearing the zoning database from the switch is the Reset Zoning command.

edit
Opens a Zoning Edit session.

history
Displays a history of zoning modifications including the following:

- Time of the most recent zone set activation or deactivation and the user who performed it
- Time of the most recent modifications to the zoning database and the user who made them.
- Checksum for the zoning database

limits
Displays the number of zone sets, zones, aliases, members per zone, members per alias, and total members in the zoning database. This keyword also displays the zoning database limits.

list
Lists all fabric zoning definitions. This keyword is does not require an Admin session nor a Zoning Edit session.

restore
Reverts the changes to the zoning database that have been made during the current Zoning Edit session since the last Zoning Save command was entered.

save
Saves changes made during the current Zoning Edit session. The system will inform you that the zone set must be activated to implement any changes. This does not apply if you entered the Zoning Clear command during the Zoning Edit session.

Examples

The following is an example of the Zoning Edit command:

```
SANbox2 #> admin start

SANbox2  (admin) #> zoning edit

SANbox2  (admin-zoning) #>
.
.
SANbox2  (admin-zoning) #> zoning cancel

  Zoning edit mode will be canceled.  Please confirm (y/n): [n]   y

SANbox2  (admin) #> admin end
```

The following is an example of the Zoning Limits command:

```
SANbox2 #> zoning limits

  Zoning Attribute     Maximum   Current   [Name]
  ----------------     -------   -------   ------
  MaxZoneSets          256       6
  MaxZones             256       19
  MaxAliases           256       1
  MaxTotalMembers      6000      166
  MaxZonesInZoneSets   1000      19
  MaxMembersPerZone    2000
                                 10        D_1_JBOD_1
                                 23        D_1_Photons
                                 9         D_2_JBOD1
                                 16        D_2_NewJBOD_2
                                 5         E1JBOD1
                                 5         E2JBOD2
                                 3         LinkResetZone
                                 3         LinkResetZone2
                                 8         NewJBOD1
                                 8         NewJBOD2
                                 12        Q_1Photon1
                                 12        Q_2Photon2
                                 8         Q_1_NewJBOD1
                                 13        Q_1_Photon_1
                                 8         Q_2_NewJBOD2
                                 13        Q_2_Photon_2
                                 3         ZoneAlias
                                 3         ZoneDomainPort
                                 4         ZoneFCAddr
  MaxMembersPerAlias   2000
                                 2         AliasInAZone
```

The following is an example of the Zoning List command:

```
SANbox2 #> zoning list

  Active ZoneSet Information

  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f

              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31

              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16

              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:c3

  Configured Zoning Information

  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f

              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
```

```
wwn_221416
          50:06:04:82:bf:d2:18:c2
          50:06:04:82:bf:d2:18:d2
          10:00:00:00:c9:22:14:16

wwn_2215c3
          50:06:04:82:bf:d2:18:c2
          50:06:04:82:bf:d2:18:d2
          10:00:00:00:c9:22:15:
```

Notes

Glossary

Access Control List Zone

Access Control List zoning divides the fabric for purposes of controlling discovery and inbound traffic.

Active Zone Set

The zone set that defines the current zoning for the fabric.

Active Firmware

The firmware image on the switch that is in use.

Activity LED

A port LED that indicates when frames are entering or leaving the port.

Administrative State

State that determines the operating state of the port, I/O blade, or switch. The configured administrative state is stored in the switch configuration. The configured administrative state can be temporarily overridden using the command line interface.

Alarm

A message generated by the switch that specifically requests attention. Alarms are generated by several switch processes. Some alarms can be configured.

Alias

A named set of ports or devices. An alias is not a zone, and can not have a zone or another alias as a member.

AL_PA

Arbitrated Loop Physical Address

Arbitrated Loop

A Fibre Channel topology where ports use arbitration to establish a point-to-point circuit.

Arbitrated Loop Physical Address (AL_PA)

A unique one-byte value assigned during loop initialization to each NL_Port on a loop.

ASIC

Application Specific Integrated Circuit

Auto Save

Zoning parameter that determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to permanent memory on that switch.

BootP

A type of network server.

Buffer Credit

A measure of port buffer capacity equal to one frame.

Cascade Topology

A fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology.

Class 2 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports wit h acknowledgment provided.

Class 3 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment.

Configured Zone Sets

The zone sets stored on a switch excluding the active zone set.

Default Visibility

Zoning parameter that determines the level of communication among ports/devices when there is no active zone set.

Device Security

A component of fabric security that provides for the authorization and authentication of devices that attach to a switch through the use of groups and security sets.

Domain ID

User defined number that identifies the switch in the fabric.

Event Log

Log of messages describing events that occur in the fabric.

Expansion Port

E_Port that connects to another FC-SW-2 compliant switch.

Fabric Database

The set of fabrics that have been opened during a SANbox Manager session.

Fabric Device Management Interface

An interface by which device host bus adapters can be managed through the fabric.

Fabric Management Switch

The switch through which the fabric is managed.

Fabric Name

User defined name associated with the file that contains user list data for the fabric.

Fabric Port

An F_Port or FL_Port.

Fabric Security

The functions that provide security for fabric users and devices including device security, user account security, and fabric services.

Fabric Services

A component of fabric security that provides for the control of inband management and SNMP on a switch.

Fabric View File

A file containing a set of fabrics that were opened and saved during a previous SANbox Manager session.

Fan Fail LED

An LED that indicates that a cooling fan in the switch is operating below standard.

FDMI

See Fabric Device Management Interface.

Flash Memory

Memory on the switch that contains the chassis control firmware.

Force PROM Mode

See Maintenance Mode.

Frame

Data unit consisting of a start-of-frame (SOF) delimiter, header, data payload, CRC, and an end-of-frame (EOF) delimiter.

FRU

Field Replaceable Unit

Group

A list of device worldwide names that are authorized to attach to a switch. There are three group types: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS).

Heartbeat LED

A chassis LED that indicates the status of the internal switch processor and the results of the Power-On Self-Test.

Inactive Firmware

The firmware image on the switch that is not in use.

Inband Management

The ability to manage a switch through another switch over an inter-switch link.

Initiator

The device that initiates a data exchange with a target device.

In-Order-Delivery

A feature that requires that frames be received in the same order in which they were sent.

Input Power LED

A chassis LED that indicates that the switch logic circuitry is receiving proper DC voltages.

Inter-Switch Link

The connection between two switches using E_Ports.

I/O Blade

Fibre Channel component of the SANbox2-64 switch.

IP

Internet Protocol

LIP

Loop Initialization Primitive sequence

Logged-In LED

A port LED on SANbox2-8c and SANbox2-16 switches that indicates device login or loop initialization status.

Maintenance Button

Formerly known as the Force PROM button. Momentary button on the switch used to reset the switch or place the switch in maintenance mode.

Maintenance Mode

Formerly known as force PROM mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes.

Management Information Base

A set of guidelines and definitions for SNMP functions.

Management Workstation

PC workstation that manages the fabric through the fabric management switch.

Mesh Topology

A fabric in which each chassis has at least one port directly connected to each other chassis in the fabric.

MIB

Management Information Base

Multistage Topology

A fabric in which two or more edge switches connect to one or more core switches.

NL_Port

Node Loop Port. A Fibre Channel device port that supports arbitrated loop protocol.

N_Port

Node Port. A Fibre Channel device port in a point-to-point or fabric connection.

Output Power LED

A power supply LED that indicates that the power supply is providing DC voltage to the switch. Applies only to SANbox2-16 and SANbox2-64 switches.

Over Temperature LED

A chassis LED or a power supply LED that indicates that the switch or power supply is overheating.

Pending Firmware

The firmware image that will be activated upon the next switch reset.

Port Status LED

A dual-function port LED on a SANbox2-64 switch that indicates device login or loop initialization status, and port activity.

POST

Power On Self Test

Power On Self Test (POST)

Diagnostics that the switch chassis performs at start up.

Principal Switch

The switch in the fabric that manages domain ID assignments.

SANbox Manager

Switch management application.

Security Set

A set of up to three groups with no more than one of each group type: ISL, Port, or MS. The active security set defines the device security for a switch.

SFP

Small Form-Factor Pluggable.

Small Form-Factor Pluggable

A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the Fibre Channel port.

SNMP

Simple Network Management Protocol

Soft Zone

Soft zoning divides the fabric for purposes of controlling discovery. Members of the same soft zone automatically discover and communicate freely with all other members of the same zone.

Target

A storage device that responds to an initiator device.

User Account

An object stored on a switch that consists of an account name, password, authority level, and expiration date.

User Account Security

A component of fabric security that provides for the administration and authentication of account names, passwords, expiration dates, and authority level.

VCCI

Voluntary Control Council for Interference

Virtual Private Fabric Zone

Virtual Private Fabric zoning divides the fabric for purposes of controlling discovery and both inbound and outbound traffic.

Worldwide Name (WWN)

A unique 64-bit address assigned to a device by the device manufacturer.

WWN

Worldwide Name

Zone

A set of ports or devices grouped together to control the exchange of information.

Zone Set

A set of zones grouped together. The active zone set defines the zoning for a fabric.

Zoning Database

The set of zone sets, zones, and aliases stored on a switch.

Notes

Index

Numerics

10/100 Base-T straight cable 4-9

A

access 3-8
Access Control List zone 3-9
account name
  default B-1
  description 3-11
  display B-90
  ftp 5-4
  maintenance mode 5-13
Activity LED 2-5
Admin
  account name B-3
  authority B-3
Admin command B-4
administrative state
  port B-53
  switch B-38
air flow 2-10, A-4
alarm
  configuration B-43
  configuration display B-72
  log B-37, B-59
alias
  add members B-5
  copy B-5
  create B-5
  delete B-5
  delete members B-6
  display list B-5
  display members B-6
  rename B-6
Alias command B-5
altitude A-4
Arbitrated Loop Physical Address B-53
authentication
  device 3-11, B-12
  user 3-11
authority 3-11, B-3

B

bandwidth 3-7
beacon B-37
binding B-12
brackets 4-2, 4-4
broadcast B-59
browser 4-1
buffer credit 3-6, A-2

C

cable
  10/100 Base-T 4-9
  10/100 Base-T crossover 4-9
  fibre optic 3-1
  null modem F/F DB9 4-9
cascade topology 3-3
CHAP authentication B-12
chassis
  air flow A-4
  diagnostics 5-9
  LEDs 2-3
  marking A-5
  shock A-4
  status B-59
  vibration A-4
classes of service A-1
Command Line Interface B-1
command syntax B-2
commands B-3
Config command B-7
configuration
  activate B-7
  backup B-7
  copy B-7
  delete B-7
  edit B-7
  file 5-3
  file system error 2-2, 5-2

list B-7
remove 5-14
reset B-27
restore B-8
restore default 5-14
save B-8
controls 2-2
credits 3-6, A-2

D

Date command B-10
device
cabling 4-16
description 3-1
device security 3-11
diagnostics 5-1, 5-9, A-2
dimensions A-3
disk space 4-1
distance 3-6
domain ID 5-6, B-12
description 3-2
lock 3-2
domains B-60
donor port 3-6, B-60

E

E_Port 2-7, 5-6
emissions standards A-5
environmental
conditions 4-2
specifications A-4
Ethernet
connection 4-10
direct connection 4-9
indirect connection 4-9
port 2-7
event logging
by component B-50, B-75
by port B-51, B-75
by severity level B-75
display B-75
restore defaults B-51
save settings B-51
settings B-75
severity level B-51
start B-51
stop B-52
external test B-83

F

F_Port 2-7
fabric
aggregate bandwidth A-2
latency A-2
management 3-16, A-3
management switch 2-7
management workstation 4-1
point-to-point bandwidth A-2
ports 2-7
security 3-10
services 3-15
Fabric Device Management Interface B-60
factory defaults 5-14, B-27
Fallback command B-11
Fan Fail LED 2-3, 5-10
fans 2-10, 6-4
fatal error 5-1, 5-2
fiber optic cable 3-1
Fibre Channel
ports 2-4
protocols A-1
field replaceable unit 6-1
File Transfer Protocol 4-19, 5-3
firmware
display versions 5-15
failure 5-2
image 5-15
image file B-21
install with CLI 4-18
install with FTP and CLI 4-19
install with SANbox Manager 4-17
list image files B-21
non-disruptive activation B-20
pending 5-15, B-11
remove image files B-21
retrieve image file B-21

unpack image 5-14, B-21
version B-64
FL_Port 2-7
flash memory 2-2, 4-20
frame size A-2
FRU - See Field Replaceable Unit
FTP - See File Transfer Protocol

G

G_Port 2-7
GBIC - See GigaBit Interface Converter
generic ports 2-6
Gigabit Interface Converter 3-1
GL_Port 2-6
group
add member B-12
copy B-13
create B-13
description 3-11
edit member attributes B-13
list B-13
list members B-14
remove member B-14
rename B-14
type B-13
Group command B-12

H

Hardreset command B-16
harmonics A-5
HBA - See Host Bus Adapter
Heartbeat LED 2-4, 5-1
heat output A-3
Help command B-17
History command B-19
host bus adapter 3-1, B-60
Hotreset command B-20
humidity 4-2, A-4
HyperTerminal application 4-10

I

Image command B-21
immunity A-5
inband management 3-15
Input Power LED 2-4, 5-10
installation 4-2
internal
firmware failure 5-2
test B-83
internet browser 4-1
ISL group 3-11, B-13

L

laser specifications A-7
latency 3-7, A-2
LED
Activity 2-5
Fan Fail 2-3, 5-10
Heartbeat 2-4, 5-1
Input Power 2-4, 5-10
Logged-In 2-5, 5-5
Output Power 2-9, 5-11
Over Temperature (chassis) 2-3, 5-10
Over Temperature (power supply) 2-9, 5-11
link state database B-60
Lip command B-22
log
archive B-50
clear B-50
copy 5-14
event B-50, B-75
power-on self test B-63
logged in users B-64
Logged-In LED 2-5, 5-5
login limit 3-16, B-1
loop port
bypass B-53
enable B-53
initialization B-22

M

maintainability A-2
maintenance
blink pattern 5-2
exit 5-13
interface A-3

menu 5-13
mode 2-2, 5-2, 5-12
strategy A-2
Maintenance button 2-2, 5-12
management
server group B-13
workstation 2-7, 4-9
manufacturer information B-79
marking A-5
MD5 authentication B-12
media type A-2
memory 4-1
activity B-60
flash 2-2
mesh topology 3-4
minicom 4-11
MS group 3-11, B-13
Multistage topology 3-5

N

name server
display B-60
zone 3-9
network
configuration reset B-28
interfaces B-60
non-disruptive activation B-20
non-fatal error 5-1
null modem F/F DB9 cable 4-9

O

online test B-83
operating systems 4-1
Output Power LED 2-9, 5-11
Over Temperature LED
chassis 2-3, 5-10
power supply 2-9, 5-11

P

page break B-37
Passwd command B-23
password 3-11
change B-23
file reset 5-14
maintenance mode 5-13
restore default 5-14
switch B-23
user account B-1
pending firmware 5-15
performance 3-6
Ping command B-24
planning 3-1
port
administrative state B-53
buffer credits 3-6
configuration 4-16, B-39
configuration display B-72
counters B-53
diagnostics 5-5
Ethernet 2-7
external test B-83
Fibre Channel 2-4
generic 2-6
group 3-11, B-13
initialize B-27
internal test B-83
LEDs 2-5
loopback test B-83
maximum number of ports/users A-1
modes 2-6
online test B-83
operational information B-61
performance B-61, B-77
serial 2-8
speed A-2, B-53
POST - See Power On Self Test
power
consumption A-3
cords 4-2
down switch 4-20
requirements 4-1
source loading A-3
supply 2-9, 6-3
switch 2-2
power on self test
description 5-1
log B-63

results 4-8
principal
priority 3-2
switch 3-2
processor 4-1
Ps command B-25

Q

Quit command B-26

R

rack mount 4-3
recovering a switch 5-12
regulatory certifications A-5
remake filesystem 5-15
removal/replacement 6-1
Reset command B-27
RS-232 port 2-8
rubber feet 4-2

S

safety standards A-5
SANbox Manager 2-10
SANbox Manager installation
Linux 4-12, 4-15
Solaris 4-13, 4-15
Windows 4-12, 4-14
SANmark A-5
scalability A-1
secret 3-11, B-12
Security command B-32
security database
clear B-32
description 3-11
display B-33
display history B-33
limits B-33
security edit session
cancel B-32
initiate B-32
revert changes B-33
save changes B-33
security set
activate B-35
add member group B-35
copy B-35
create B-35
deactivate B-35
delete B-36
delete member group B-36
description 3-11
display B-36
display active B-32, B-35
display members B-36
rename B-36
Securityset command B-35
serial port 2-8, 4-9, 4-10
Set command B-37
Set Config command B-39
Set Log command B-50
Set Port command B-53
Set Setup command B-54
SFP - See Small Form-Factor Pluggable
SHA-1 authentication B-12
Show command B-59
Show Config command B-72
Show Log command B-75
Show Perf command B-77
Show Setup command B-79
Shutdown command B-82
Simple Network Management Protocol
configuration B-54
configuration display B-79
description 2-10
enable 3-15
reset B-27
site requirements 4-1
small form-factor pluggable 2-6, 4-5, 6-2
SNMP See - Simple Network Management Protocol
soft zone 3-9
steering B-63
switch
administrative state B-38
configuration 4-15, B-42
configuration display B-72
hard reset B-16

management 2-10
manufacturer information B-79
operational information B-64
power down 4-20
recovery 5-12
reset 2-2, 5-15, B-86
reset without POST B-27
specifications A-1
system configuration
change B-55
display B-79
system processor A-2

T

table mount 4-3
temperature 4-2, A-4, B-59
Test command B-83
time B-10
timeout value 5-6
topology
cascade 3-3
mesh 3-4
Multistage 3-5
transceiver 2-6, 4-5, 6-2
transmission rate 3-6, 3-7

U

Uptime command B-86
user
account B-1
authentication 3-11
interface A-2
logged in B-64
user account security 3-11
User command B-87

V

ventilation 2-10
vibration A-4
Virtual Private Fabric zone 3-10
voltage
fluctuations A-5
operating A-3

W

Whoami command B-90
workstation 4-1, 4-9
worldwide name 3-8
WWN - See Worldwide Name

Z

zone
access control list 3-9
add member port B-91
conflict 5-6
copy B-91
create B-91
definition 3-8
delete B-91
delete member port B-92
list B-92
list members B-92
name server 3-9
rename B-92
type B-92
virtual private fabric 3-10
Zone command B-91
zone set 3-8
activate B-95
active B-97
add member zone B-95
copy B-95
create B-95
deactivate B-27, B-28, B-95
delete B-95
delete member zone B-96
display B-96
display active B-95
display members B-96
display zones B-92
rename B-96
Zoneset command B-95
zoning
configuration B-45
configuration display B-72
database 3-8, B-27, B-28
edit B-97

history B-97
limits 3-8, B-98
list definitions B-98
revert changes B-98
save edits B-98
Zoning command B-97

Notes